Math 122—Algebra I

Lectures by Barry Mazur
Notes by Max Wang

Harvard University, Fall 2010

Introduction

Math 122 is the first in a two-course undergraduate series on abstract algebra offered at Harvard University. It primarily covers the theory of groups and rings, although it also recaps some linear algebra which is typically taught in greater detail during freshman year.

These notes were live-TEXed, then edited for correctness and clarity. I am responsible for all errata in this document, mathematical or otherwise; any merits of the material here should be credited to the lecturer, not to me.

Feel free to email me at mxawng@gmail.com with any comments.

Acknowledgments

In addition to the course staff, acknowledgment goes to Zev Chonoles, whose online lecture notes (`http://math.uchicago.edu/~chonoles/expository-notes/`) inspired me to post my own. I have also borrowed his format for this introduction page.

The page layout for these notes is based on the layout I used back when I took notes by hand. The LATEX styles can be found here: `https://github.com/mxw/latex-custom`.

Copyright

Lecture 1 — 9/16/10

Definition 1.1. A composition law or multiplication law on a set S is a map $c : S \times S \to S$.

Example. (Composition of functions)
Let X be a set. Define $S := \{f : X \to X\}$. Consider the map

$$S \times S \to S$$
$$(f, g) \mapsto f \circ g$$

given by $(f \circ g)(x) = f(g(x))$. Note that $\circ$ is associative:

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$$
$$h \circ (g \circ f) = (h \circ g) \circ f$$

Definition 1.2. A group is a set G with composition law $\cdot$ satisfying

1. associativity
2. two-sided identity: $\forall g \in G, \exists 1 \in G :$
$$g \cdot 1 = g = 1 \cdot g$$
3. inverse law: $\forall g \in G, \exists g^{-1} \in G :$
$$g \cdot g^{-1} = 1 = g^{-1} \cdot g$$

Proposition 1.3. *g^{-1} is unique.*

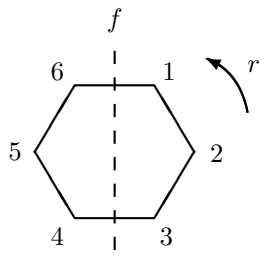
Proof. Suppose $g, g_1^{-1}, g_2^{-1} \in G$, where g_1^{-1}, g_2^{-1} both inverses g.

$$\begin{aligned} 1 &= g_1^{-1} \cdot g \\ 1 \cdot g_2^{-1} &= (g_1^{-1} \cdot g) \cdot g_2^{-1} \\ g_2^{-1} &= g_1^{-1} \cdot (g \cdot g_2^{-1}) \\ g_2^{-1} &= g_1^{-1} \end{aligned}$$

■

Definition 1.4. The order of a group G, denoted $|G|$, is the cardinality of the set G.

Example. Consider the group of symmetries of regular n-gon, which is given by the group D_{2n}, the dihedral group of order $2n$. Consider the regular hexagon:



where r = rotation by $\frac{360^\circ}{n}$ and f = flip across axis (note that rotation rotates this axis of reflection), and these two functions are related by function composition. Note that both r and f permute the vertices of the hexagon (so, for instance, $f(r(1,2,3,4,5,6)) = (2,3,4,5,6,1) = (5,4,3,2,1,6)$). We also have that $r^n = 1, f^2 = 1, fr = r^{-1}f$ for D_{2n}.

Example. The symmetric group or the permutation group on n "letters" is

$$S_n := \{\text{bijections } \{1, \dots, n\} \longleftrightarrow \{1, \dots, n\}\}$$

The composition law on S_n is function composition, and $|S_n| = n!$.

Example. The general linear group is $GL_n(\mathbb{R})$, the group of invertible n-by-n real matrices with matrix multiplication as the composition law.

Definition 1.5. Let G be a group, $H \subseteq G$. Then H is a subgroup of G if H is closed under composition and inversion and if $1 \in H$. We write $H \leq G$.

Example. $\quad D_{2n} \subseteq S_n \qquad D_6 = S_3$

Definition 1.6. Two groups $(G_1, \cdot), (G_2, \odot)$ are homomorphic if $\exists \varphi : G_1 \to G_2$ such that $\forall x, y \in G$, $\varphi(x \cdot y) = \varphi(x) \odot \varphi(y)$. h is called a homomorphism. A bijective homomorphism is called an isomorphism, and G_1, G_2 are isomorphic in that case.

Example.

$$r := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, f := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\left(\{\textstyle\prod A : A = r, f \in GL_n(\mathbb{R})\}, \cdot\right) \cong D_6$$

Definition 1.7. An abelian group is a group whose composition law satisfies

4. commutativity

Note. If G a group, $\forall a, b, c \in G, c \cdot a = b \cdot a \iff c = b$. This is called the cancellation law.

Lecture 2 — 9/7/10

Proposition 2.1. *Let G be a group, $H \subseteq G$. $H \leq G$ iff H is nonempty and closed under $(a, b) \mapsto a \cdot b^{-1}$.*

Lemma 2.2. *The intersection of any collection of subgroups of G is again a subgroup.*

Example.

1. The functions $\mathbb{R}^+ \underset{\ln x}{\overset{e^x}{\rightleftarrows}} \mathbb{R}^{>0}$ (from the reals under $+$ to the positive reals under $\cdot$). We have $e^{x+y} = e^x \cdot e^x$ and $\ln(x \cdot y) = \ln(x) + \ln(y)$, so both are homomorphic; since they are also inverses, $\mathbb{R}^+ \cong \mathbb{R}^{>0}$.

2. $\mathbb{Z}^+ - \{0\}$ is closed under associative $\cdot$ with an identity element, but fails to follow the inverse law; however, the cancellation law still holds.

Lemma 2.3. *Let $\varphi : G_1 \to G_2$ be a homomorphism between groups. Then $\mathrm{im}(\varphi)$ is a subgroup of G_2.*

Proof. $\varphi(1_1) = 1_2$, and $\forall x \in G_1, \varphi(x^{-1}) = \varphi(x)^{-1}$. ■

Note. Let $\varphi : G_1 \to G_2$ be a homomorphism between groups, $x \in G_1$.

1. $\varphi(x^n) = \varphi(x)^n, \forall n \in \mathbb{Z}$
2. $x^0 := 1_1 \implies \varphi(x)^0 = 1_2$
3. $n = -m \implies x^n = (x^{-1})^m = (x^m)^{-1}$

Definition 2.4. Let G a group, $a \in G$. Define $F_a : \mathbb{Z}^+ \to G$ by $n \mapsto a^n$. Since $\forall n, m \in \mathbb{Z}$, $a^{n+m} = a^n \cdot a^m$, F_a is a homomorphism. Then the subgroup of G generated by a is defined

$$\langle a \rangle := \mathrm{im}(F_a) = \{a^n\}$$

We write $\mathrm{ord}(a) = |a| = |\langle a \rangle|$.

Definition 2.5. Let $S \subseteq G$ a group. Then the subgroup of G generated by S is

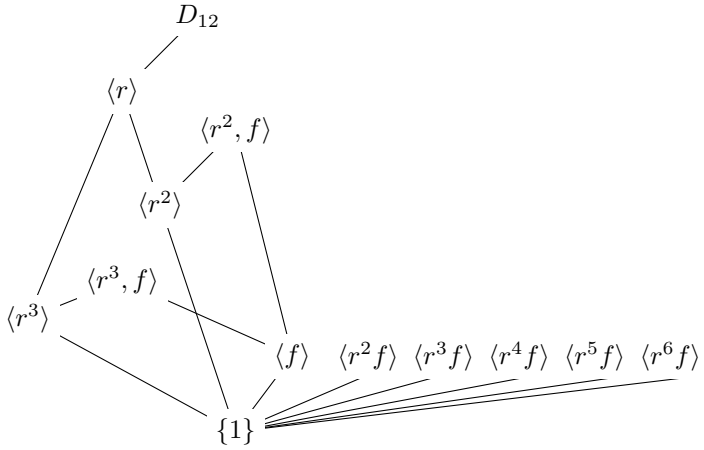
$$\langle S \rangle := \bigcap_{\substack{H \leq G: \\ S \subseteq H}} H$$

Remark.

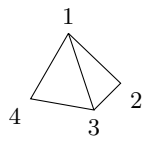
1. There is at least one subgroup of G containing S, namely G.
2. By lemma, the intersection is a subgroup of G.
3. Any subgroup of G containing S contains $\langle S \rangle$.
4. $\langle S \rangle$ is the smallest subgroup containing S.

Example. $\langle r, f \rangle = D_{2n}$. We say that r, f are generators of D_{2n}.

Example. Lattice of subgroups of D_{12}.



Example. Let G be the group of symmetries of the regular tetrahedron.



The map $G \ni g \mapsto P_g \in S_4$ is an injective homomorphism of groups

$$G \longrightarrow\!\!\!\!\!\rightarrow S_4$$

Example. Find a surjective homomorphism

$$S_4 \longrightarrow\!\!\!\!\!\rightarrow S_3$$

The regular tetrahedron has 6 edges, in which there are three pairs of opposite edges. Any permutation of $\{1, \ldots, 4\}$ brings edges to edges:

$$\{\text{edge, opp edge}\} \longrightarrow \{\text{edge', opp edge'}\}$$
$$\{(12), (34)\} \longrightarrow \{(1'2'), (3'4')\}$$

Each permutation of $\{1, \ldots, 4\}$ gives a permutation of $\{I, II, III\}$, sets of opposite edges.

Lecture 3 — 9/9/10

Note. Let $\mathbb{Z}^+$ be the additive group of integers, and let $H \leq \mathbb{Z}^+$. Either $H = \{0\}$ or H contains a positive number.

Observation 3.1. Let d be the smallest positive element in H. Then every element of H is a multiple of d; that is,

$$\langle d \rangle = H = \{0, \pm d, \pm 2d, \ldots\} = \{n \cdot d : n \in \mathbb{Z}\} =: d \cdot \mathbb{Z}$$

Proof. Let $a \in H, a > 0$. Then $a = m \cdot d + r$, $0 \leq r < d$. $a \in H, d \in H \implies r = a - md \in H$. Either $r = 0$ or $0 < r < d$. $r = 0 \implies a$ a multiple of d. $r \neq 0 \implies r < d$. But $r \in H$ where d is minimal. $\Rightarrow\Leftarrow$. ■

Proposition 3.2. *Let* $\text{slc}(a,b)$ *denote the smallest positive linear combination of* a, b*. Then* $\forall a, b \in \mathbb{Z}, a, b > 0$, $\gcd(a,b) = \text{slc}(a,b)$*. Moreover,* $\gcd(a,b)$ *is the only common divisor of* a, b *that is a linear combination, and* $\text{slc}(a,b)$ *is the only linear combination of* a, b *that is also a common divisor. Furthermore, any linear combination of* a, b *is a multiple of* $\text{slc}(a,b)$*.*

Proof. The set of all linear combinations of a, b is given by

$$\text{LC}(a,b) := \{ar + bs : r, s \in \mathbb{Z}\} = \langle a, b\rangle = \langle d\rangle \subset \mathbb{Z}^+$$

for some d, by the previous observation. Since $\langle d\rangle = \langle a, b\rangle$, we must have $d|a$ and $d|b$. We also have that

$$d = aR + bS : R, S \in \mathbb{Z}$$

Let c be a common divisor of a, b: $c|a$ and $c|b$. Then $c|aR + bS \implies c|d \implies d = \gcd(a,b)$. (Note that we have also shown that any common divisor of a, b divides $\gcd(a,b)$. ∎

Definition 3.3. A <u>finite cyclic group</u> of order n is a group C_n with the property that $C_n = \langle x\rangle$ for some $x \in C_n$, and n is the smallest number such that $x^n = 1$.

$$C_n = \langle x\rangle = \{1, x, x^2, \ldots, x^{n-1}\}$$

Claim 3.4. *Let* $H \subseteq C_n$ *be a subgroup,* $H \neq \{1\}$*. Then the subset* $S \subset \mathbb{Z}^+$ *defined*

$$S := \{a \in \mathbb{Z}^+ : x^a \in H\}$$

is a subgroup of $\mathbb{Z}^+$*.*

Proof. Let $a, b \in S$. Then $x^a, x^b \in H$. Since H is closed under $\cdot$, $x^a \cdot x^b = x^{a+b} \in H \implies a + b \in S$. Since H is closed under inverse, $(x^a)^{-1} = x^{-a} \in H \implies -a \in S$. Finally, $1 = x^0 \in H \implies 0 \in S$. ∎

Proposition 3.5. *Any subgroup of* C_n *is generated by* x^d *for some* $d|n$*. Furthermore,* $\{H : H \subseteq C_n \text{ a subgroup}\}$ *is bijective with the set* $\{d : d|n\}$*.*

Proof. Recall S above. Since S is a subfield of $\mathbb{Z}^+$, $S = \langle d\rangle$ for some d. Hence,

$$H = \{1, x^{\pm d}, x^{\pm 2d}\}$$

We have that $x^n = 1 \in H \implies n \in S \implies d|n$. ∎

Note.

$$\begin{aligned} \mathbb{Z}^+ &\twoheadrightarrow C_n \\ a &\longmapsto x^a \end{aligned}$$

Definition 3.6. The <u>circle group</u> is given by

$$\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$$

Note that every point in $\mathbb{T} \iff$ some angle θ, and that multiplication of points $\iff$ adding angles. The circle group is also abelian. Note that

$$\begin{aligned} \mathbb{R}^+ &\twoheadrightarrow \mathbb{T} \\ r &\longmapsto e^{2\pi i r} \end{aligned}$$

and also that

$$\begin{aligned} C_n &\twoheadrightarrow \mathbb{T} \\ x^a &\longmapsto e^{2\pi i \frac{1}{n}} \end{aligned}$$

Lecture 4 — 9/14/10

Definition 4.1. An <u>automorphism</u> is an isomorphism from a group G to itself.

Proposition 4.2. *For any group* G*, the set of all automorphisms on* G*, denoted* $\text{Aut}(G)$*, is a group.*

Proof. The identity function serves as the identity element in $\text{Aut}(G)$, function composition is associative, and since automorphisms are bijective, each function clearly has an inverse in $\text{Aut}(G)$. ∎

Definition 4.3. Let $g \in G$ a group. The <u>conjugation</u> by g is the map $c_g : G \to G$ given by $x \mapsto gxg^{-1}$.

Proposition 4.4. c_g *as defined above is an automorphism. The set of all automorphisms* c_g *is a group*

$$\text{Inn}(G) \subseteq \text{Aut}(G)$$

called the <u>inner automorphism group</u>. Moreover, the map $c : G \to \text{Inn}(G)$ *given by* $c(g) = c_g$ *is a group homomorphism, and* G *is abelian iff* c *is trivial.*

Proof. Let $x, y \in G$.

$$c_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = c_g(x)c_g(y)$$

So c_g is a homomorphism. Surjectivity is obvious; $\forall x \in G, c_g(g^{-1}xg) = x$. Finally, let $x, y \in G, x \neq y$. If $c_g(x) = c_g(y)$, then

$$g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g$$

So $x = y$. Then c_g is injective, and hence an automorphism.

Conjugation by 1 yields the identity automorphism, and the composition $c_g \circ c_{g'}$ yields conjugation by gg', and hence $\text{Inn}(G)$ is indeed a group. Now fix $x \in G$. Let $g, g' \in G$.

$$c(gg')(x) = c_{gg'}(x) = gg'xg'^{-1}g^{-1} = c_g(c_{g'}(x)) = c_g \circ c_{g'}(x)$$

So c is indeed a group homomorphism.

Suppose G is abelian. Then

$$c_g(x) = gxg^{-1} = xgg^{-1} = x$$

and hence $c_g \equiv \text{id}$. If $\forall g \in G, c_g \equiv \text{id}$, then $gxg^{-1} = x = xgg^{-1} \implies gx = xg$, and hence G is abelian. ■

Definition 4.5. A subgroup $N \subseteq G$ is normal in G if $\forall g \in G, \forall n \in N, g \cdot n \cdot g^{-1} \in N$. We write $N \trianglelefteq G$.

Definition 4.6. The kernel of a homomorphism $\varphi : G \to G'$ between groups is

$$\ker(\varphi) := \{x \in G : \varphi(x) = 1\}$$

Proposition 4.7. *Given $\varphi : G \to G'$ a group homomorphism,*

1. $\ker(\varphi)$ *is a subgroup.*
2. $\ker(\varphi)$ *is normal.*

Proof.

1. Let $g, g' \in \ker(\varphi)$. Then $\varphi(gg') = \varphi(g)\varphi(g') = 1$, and hence $\ker(\varphi)$ is closed under multiplication. It is clear that $1 \in \ker(\varphi)$, and since

   $$1 = \varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(g^{-1})$$

   $\ker(\varphi)$ is closed under inverse, and hence is a subgroup.

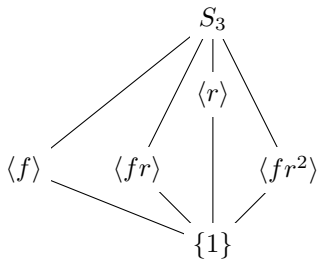
2. Let $n \in \ker(\varphi), g \in G$.

   $$\varphi(gng^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(k) = 1$$

   so $gng^{-1} \in \ker(\varphi)$, which means that $\ker(\varphi)$ is normal. ■

Definition 4.8. Let G be a group, $g \in G$, $H \subseteq G$ a subgroup. Conjugation of all elements in H with g yields a conjugate subgroup gHg^{-1}.

Example. Consider the lattice of subgroups of S_3.



The subgroup $\langle r \rangle$ is normal (and $\langle r \rangle \cong C_3$). However, none of the subgroups $\langle f \rangle, \langle fr \rangle, \langle fr^2 \rangle$ are normal, and conjugation with any element in G yields another one of the subgroups.

Definition 4.9. Let G be a group. The center of G is the set

$$Z(G) = \{z \in G : \forall g \in G, z \cdot g = g \cdot z\}$$

Proposition 4.10. *Let G be a group, $c : G \to \text{Inn}(G)$ be given by $g \mapsto c_g$. Then $Z(G) = \ker(c)$.*

Proof. Let $g \in \ker(c)$. Then $c(g) = \text{id}$, or equivalently, $c_g(x) = x, \forall x \in G$. Then $gxg^{-1} = x = xgg^{-1}$, and by cancellation, $gx = xg$, so $g \in Z(G)$. Now let $g \in Z(G)$. Then $c_g(x) = gxg^{-1} = xgg^{-1} = x$, so $c_g \equiv \text{id}$ and $g \in \ker(c)$. ■

Corollary 4.11. *$Z(G)$ is normal.*

Definition 4.12. Let G be a group, $H \subseteq G$ a subgroup. Fix $h \in H$. The map $G \to G$ given by $x \mapsto x \cdot h$ is clearly bijective. Define a relation $x \sim y$ iff $\exists h \in H : y = x \cdot h$. It is easily seen that this is an equivalence relation on G:

1. $x \sim x \iff x = xh \iff h = 1$
2. $x \sim y \iff x = yh \iff y = xh^{-1} \iff y \sim x$.
3. $x \sim y, y \sim z \iff x = yh, y = zh' \iff x = zh'h \iff x \sim z$.

This equivalence relation yields a natural partition of the set G into disjoint unions of left H-cosets

$$gH = \{gh : h \in H\}$$

We can also similarly define right H-cosets by

$$Hg = \{hg : h \in H\}$$

Lecture 5 — 9/16/10

Remark. We can view a left H-coset in terms of a representative of the coset. Given $x \in gH$, every element in gH has the form $xh : h \in H$. We can see that any two left H-cosets in G are bijective

$$\{xh : h \in H\} \longleftrightarrow \{yh : h \in H\}$$

and in particular, we have a bijection $z \mapsto (x^{-1}y) \cdot z$. This means that $|gH|$ does not depend on g, and moreover, $|gH| = |H|$ since $H = 1H$, the trivial coset. We can therefore write G as a disjoint union of left cosets

$$G = 1H \sqcup g_1H \sqcup g_2H \sqcup \dots$$

Note also that the number of left H-cosets and the number of right H-cosets are both equal to $|G|/|H|$.

Definition 5.1. The index $[G : H]$ of a subgroup H in a finite group G is the ratio $\frac{|G|}{|H|}$.

Theorem 5.2 (Lagrange)**.** *If G is a finite group and $H \subseteq G$ a subgroup, $|H|$ divides $|G|$. In other words,*

$$|G| = [G : H]|H|$$

Corollary 5.3. *Any group of order $p \in \mathbb{P}$ is cyclic.*

Proposition 5.4. *Let $\varphi : G \to G'$ be a group homomorphism and let $g, g' \in G$. Then $\varphi(g) = \varphi(g') \iff \exists n \in \ker(\varphi) : g' = gn$.*

Proof. Suppose $\varphi(g) = \varphi(g')$. Then $\varphi(g)^{-1}\varphi(g') = 1$, and hence $\varphi(g'^{-1}g) = 1$, so $g'^{-1}g \in \ker(\varphi)$, yielding the desired result. In the reverse direction, $g' = gn \implies \varphi(g') = \varphi(gn) \implies \varphi(g') = \varphi(g)$. ■

Note. The above proposition shows that there is a bijection between the $\ker(\varphi)$-cosets in G and $\operatorname{im}\varphi$.

Corollary 5.5. *Let $\varphi : G \to G'$ be a group homomorphism.*

$$|G| = |\ker\varphi||\operatorname{im}\varphi|$$

Definition 5.6. The set of left H-cosets in G is written G/H; that is, $c \in G/H \iff c = gH \subseteq G$ for some g. The set of right H-cosets is $H\backslash G$. We refer to these as the coset spaces.

Proposition 5.7. *Let G be a group, $H \leq G$. Let gH be a left coset and Hg' a right coset. If $gH = Hg'$, then $gH = Hg$.*

Proof. By assumption, $\exists h \in H : g1 = hg'$. Choose $h' \in H$. Then $h'g = h'hg' \in Hg'$. Similarly, $h'g' = h'h^{-1}g \in Hg$. This yields $Hg \subseteq Hg' \subseteq Hg$. Then $Hg' = Hg = gH$, as desired. ■

Proposition 5.8. *Let G be a group, $N \leq G$. Then N is normal in G iff $\forall g \in G, gN = Ng$.*

Proof. Suppose N is normal, fix $g \in G$. Then $\forall n \in N$, $gng^{-1} \in N$ and $g^{-1}ng \in N$. We have $gN \ni gn = (ghg^1)g \in Ng$ and $Ng \ni ng = g(g^{-1}ng) \in gN$, so $gN = Ng$. Suppose instead that $\forall g \in G, gN = Ng$. Fix $g \in G$. Then $gn \in gN$, and $\exists n' : Ng \ni n'g = gn$. Then $n' = gng^{-1} \in N$, so N is normal. ■

Example. Any subgroup $H \subseteq \mathbb{Z}$ is of the form

$$H = n \cdot \mathbb{Z}, n \geq 0$$

Every H coset looks like $a + n \cdot \mathbb{Z}$. $a, b \in \mathbb{Z}$ are in the same coset iff

1. $n|a - b$.
2. $a \equiv b \pmod{n}$

Note also that $\mathbb{Z}/n\mathbb{Z} \cong C_n$ and $|\mathbb{Z}/n\mathbb{Z}| = n$.

Definition 5.9. Let G be a group. Let $x \equiv y$ iff $\exists g \in G : x = gyg^{-1}$. We refer to x and y as conjugate. This achieves a partition of G into conjugacy classes, given by

$$C_x := \{gxg^{-1} : g \in G\}$$

for any $x \in G$.

Observation 5.10 (Class Equation)**.** Since all elements of $Z(G)$ the center of G commute with all other elements of G, the equivalence relation condition $x = gyg^{-1}$ yields $x = y$. Hence, every element of $Z(G)$ is in its own conjugacy class. Since the conjugacy classes partition G, we have the following class equation:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |C_x|$$

This allows us to write $|G|$ as a sum of its divisors.

Definition 5.11. An action of the group G on the set X is a map $\alpha : G \times X \to X$ satisfying

1. $\forall x \in X, \alpha(1, x) = x$
2. $\alpha(g_1 \cdot g_2, x) = \alpha(g_1, \alpha(g_2, x))$

The second axiom can also be written as an associative law: $(g_1 \cdot g_2) \odot x = g_1 \odot (g_2 \odot x)$ where $\cdot$ is group composition and $\odot$ is group action. Restricting to a single $g \in G$ yields $\alpha_g : X \to X$, which is invertible by the inverse law and the second axiom of the group action definition.

Definition 5.12. Define

$$\operatorname{Perm}(X) := \{f : X \to X | f \text{ bijective}\}.$$

An action of G on X is a homomorphism $A : G \to \operatorname{Perm}(X)$.

Claim 5.13. *The two definitions of action are equivalent.*

Proof.

$\implies$ Let $\alpha : G \times X \to X$ be an action by the first definition. We know that $\alpha_g \in \operatorname{Perm}(X)$. Then the map A given by $g \mapsto \alpha_g$ takes $G \to \operatorname{Perm}(X)$. We must show that A is a homomorphism. $1 \cdot x = x \implies A(1) = \alpha_1 = \mathrm{id}$. By "associativity," for any $x \in X$,

$$\begin{aligned} A(g_1g_2)(x) = \alpha_{g_1g_2}(x) &= (g_1g_2) \odot x \\ &= g_1 \odot (g_2 \odot x) \\ &= \alpha_{g_1}(\alpha_{g_2}(x)) \\ &= A(g_1) \cdot A(g_2)(x) \end{aligned}$$

So $\forall x \in X, A(g_1g_2) = \alpha_{g_1} \cdot \alpha_{g_2}$.

$\impliedby$ Left as exercise. ■

Lecture 6 — 9/21/10

Definition 6.1. Let α be a group action of G on X. If $x \in X$, we say that $y \in X$ is in the same orbit as x with respect to α if $\exists g \in G : g \cdot x = y$. The orbit of x is denoted

$$O_x = Gx = \{gx : g \in G\}$$

This yields an equivalence relation, which produces a set of equivalence classes X/G called the orbit space, along with a partition

$$X = \coprod_{O \in X/G} O$$

Note that

$$|X| = \sum_{O \in X/G} |O|$$

Example. A subgroup $H \subseteq G$ acts on G by left multiplication.

$$G = \coprod_{gH \in G/H} gH$$

So $|G| = |H| \cdot [G : H]$ by the rule above.

Example. Let $H \subseteq G$ be a subgroup.

1. Action by Left-μ:

$$\begin{aligned} H \times G &\longrightarrow G \\ (h, g) &\longmapsto hg \end{aligned}$$

2. Action by Right-μ:

$$\begin{aligned} H \times G &\longrightarrow G \\ (h, g) &\longmapsto gh^{-1} \end{aligned}$$

   Note that $(h, g) \mapsto gh$ fails associativity.

3. Action by Conjugation:

$$\begin{aligned} H \times G &\longrightarrow G \\ (h, g) &\longmapsto hgh^{-1} \end{aligned}$$

   We also get $H \to \mathrm{Aut}(G)$.

Note. Orbits under left or right multiplication are right and left H-cosets respectively, so all have cardinality $|H|$. Orbits under conjugation are the conjugacy classes of G.

Definition 6.2. A group action α is transitive on X if there is only one orbit: $\forall x, y \in X, \exists g \in G : g \cdot x = y$.

Definition 6.3. A fixed point under an action α is an element $x \in X : \forall g \in G, g \cdot x = x$.

Definition 6.4. Let $\alpha : G \to X$ be a group action. The stabilizer or isotropy subgroup of $x \in X$ is

$$G_x := \{g \in G : gx = x\}$$

More generally, if $S \subseteq X$, the stablizer G_S of S is

$$G_S := \{g \in G : gS = S\}$$

Lemma 6.5. *G_x is a subgroup of G.*

Proof.

1. $1 \in G_x$ because $1 \cdot x = x$.
2. Let $g_1, g_2 \in G_x$. $(g_1 \cdot g_2)(x) = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$. So $g_1 \cdot g_2 \in G_x$.
3. Let $g \in G_x$. Since $g \cdot x = x$ and $1 \cdot x = (g^{-1} \cdot g) \cdot x = x$, we have $x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$. Hence, $g^{-1} \in G_x$. ■

Lemma 6.6. *Let $x \in X$, a set acted on by a group G. Then there is a natural bijection*

$$\begin{aligned} \varphi : G/G_x &\longrightarrow O_x \\ gG_x &\longmapsto gx \end{aligned}$$

between the left G_x-coset space and the orbit of x.

Note. Take another representative $g' \in gG_x$. Then $\exists h \in G_x : g' = g \cdot h$. Since $h \in G_x$ is a stabilizer, we have

$$\begin{array}{ccc} gG_x & = & g'G_x \\ \downarrow & & \downarrow \\ g \cdot x & = & gh \cdot x = g' \cdot x \end{array}$$

This shows that our function is well-defined.

Proof. Let $g_1G_x, g_2G_x \in G/G_x$, which map to g_1x, g_2x. Suppose $g_1x = g_2x$. Then $x = g_2^{-1}g_1 \cdot x$. Call $h = g_2^{-1}g_1 \in G_x$. Then $g_2h = g_1$, so $g_1G_x = g_2G_x$. Hence, φ is injective. Our map is clearly surjective; $\forall gx \in O_x, \varphi(gG_x) = gx$. Therefore, φ is bijective. ■

Corollary 6.7 (Orbit-Stabilizer Theorem)**.** *Let G a group act on X a set, let $x \in X$.*

$$|G| = |G_x||O_x|$$

This follows from the above proposition and Lagrange's Theorem.

Example. Let $G = \mathbb{R}^+$ (note that G is abelian), let X be the unit circle in the plane. Consider the group action $\alpha(r, e^{2\pi ia}) = e^{2\pi i(a+r)}$. It is clear that $\forall x \in X, G_x = \mathbb{Z}$. The only orbit in X/G is X. Consider the G_x cosets in G. Each G_x coset is given by $r + G_x \equiv r + \mathbb{Z}$. Hence, $[0, 1) = G/G_x \to G \cdot x = X$, or $[0, 1) \ni r \equiv r + \mathbb{Z} \mapsto e^{2\pi i(a+r)}$. This is our map $g \cdot G_x \mapsto g \cdot x$.

Example. Let $G = \mathbb{R}, X = \mathbb{C}$. $r \in \mathbb{R}$ acts on $z \in \mathbb{C}$ by multiplication by $e^{2\pi ir}$. $\alpha(r, z) = e^{2\pi ir}z$. For any $z \in X, z \neq 0, G_z = \mathbb{Z}$; if $z = 0$, then $G_z = \mathbb{R}$. So the $G/G_z : z = 0$ is a single coset, namely all of $\mathbb{R}$, and the orbit of $z = 0$ consists of only 0.

Lecture 7 — 9/23/10

Example. Given a bijection $T : X \to X$, we have an action of $\mathbb{Z}$ on X given by $\alpha(n, x) = T^n(x)$, noting that $T^0 = 1, T^{-m} = (T^{-1})^m$. If we take T to be rotation by an angle $2\pi/\mathbb{Q}^C$ (that is, an angle of 2π over any irrational), $X = \mathbb{R}^2$ and choose $x \neq (0, 0)$, then the orbit of any $x \in X$ is dense within the circle of rotation of x.

Example. As an exercise, describe the automorphism group of a lattice, G, (that is, the Euclidean motions of plane bringing lattice to lattice) and the plane X.

Remark. Let $\sigma \in S_n = \text{Perm}\{1, 2, \ldots, n\}$, and let $X = \{1, \ldots, n\}$. Consider the group $\langle\sigma\rangle$ acting on X. One description of this group action (and of σ) can be given by

$$\begin{pmatrix} 1, & \ldots, & n \\ \sigma(1), \ldots, \sigma(n) \end{pmatrix}$$

We can also describe $\langle\sigma\rangle$ by the orbits of X. Consider the orbit, relative to $\langle\sigma\rangle$, of 1. $\exists d_1 : \sigma^{d_1}(1) = 1$. So the orbit of 1 is given by

$$(1, \sigma(1), \sigma^2(1), \ldots, \sigma^{d_1-1}(1))$$

Ultimately, we have

$$\sigma = (1, \sigma(1), \ldots, \sigma^{d_1-1}(1))(x_2, \sigma(x_2), \ldots, \sigma^{d_2-1}(x_2)) \cdots \cdots (x_k, \ldots, \sigma^{d_k-1}(x_k))$$

which describes σ completely (as well as the partition of X by orbits) and is unique up to (1) cyclic permutations of each of the so-called "cycles" and (2) the order of the cycles.

Definition 7.1. A permutation $\tau \in S_n$ is called a cycle of length l if $\tau = (a_1, a_2, \ldots, a_l)$, by which we mean

- $a_i \in \{1, \ldots, n\}$
- $i \neq j \implies a_i \neq a_j$
- $i < l \implies \tau(a_i) = a_{i+1}$
- $\tau(a_l) = a$
- $\tau(b) = b$ if $b \notin \{a_1, \ldots, a_l\}$

Definition 7.2. Two cycles $\tau = (a_1, \ldots, a_l)$ and $\eta = (b_1, \ldots, b_m) \in S_n$ are disjoint if $\{a_i\} \cap \{b_j\} = \emptyset$.

Note. The order of $\tau \cdot \eta = \eta \cdot \tau$ is the least common multiple of l and m.

Observation 7.3. Disjoint cycles commute.

Observation 7.4. Any permutation in S_n is expressible uniquely (up to cyclic permutation and commutativity) as a product of disjoint cycles.

Definition 7.5. A partition of a natural number $n \in \mathbb{N}$ is a collection $\{n_i \in \mathbb{N} : n_i > 0\}$ such that

$$\sum n_i = n$$

Note. A partition is associated to any $\sigma \in S_n$, where

$$\sigma = \prod_{1=0}^{t} \text{ cycles of length } n_i$$

yielding

$$n = n_1 + \ldots + n_t$$

Note that $t = |X/\langle\sigma\rangle|$ (that is, the orbits of X are fully determined by the cyclic decomposition of a permutation σ).

Note. There is a surjective map

$$\text{Part} : S_n \twoheadrightarrow \text{partitions of } n$$

Observation 7.6. Let π be a partition of n. Then

$$\text{Part}^{-1}(\pi) \subset S_n$$

Take $\sigma, \sigma' \in \text{Part}^{-1}(\pi) \subset S_n$. We can write

$$\sigma = (a_1 \cdots a_{n_1})(a_{n_1+1} \cdots a_{n_1+n_2}) \cdots (\cdots a_n)$$

and since σ, σ' induce the same partition,

$$\sigma' = (a'_1 \cdots a'_{n_1}) \cdots (\cdots a'_n)$$

There exists $g \in S_n$ such that the action of g brings

$$\begin{pmatrix} a_1, \ldots, a_n \\ a'_1, \ldots, a'_n \end{pmatrix}$$

Then it is clear that we have

$$\sigma' = g\sigma g^{-1}$$

Proposition 7.7. *Two permutations in S_n have the same partition iff they are conjugate in S_n. Hence, $\text{Part}^{-1}(\pi)$ given above is a conjugacy class in S_n.*

Definition 7.8. Let G be a group. We know that G acts on the set $X = G$ by conjugation, where $\alpha(g, x) = gxg^{-1}$. The stabilizer G_x for any $x \in X$ is called the centralizer of x, given by

$$Z(x) := \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

Observation 7.9. Let G be a group, $x \in G$. $\langle x \rangle \subseteq Z(x)$ and $\langle x \rangle \subseteq Z(Z(x))$. For any other subgroup $H \leq G$, if $x \in Z(H)$, then $H \subseteq Z(x)$.

Proposition 7.10. *Let G be a finite group, $x \in G$. Then*

$$|G| = |C_x||Z(x)|$$

follows from the Counting Formula.

Lecture 8 — 9/28/10

Corollary 8.1. *By the above proposition and the class equation,*

$$|G| = |Z(G)| + \sum [G : Z(x)]$$

Theorem 8.2. *Let G be a group, $N \leq G$. TFAE:*

1. *N is normal ($\forall g \in G, gNg^{-1} = N$).*
2. *$\forall g \in G, \exists g' : gN = Ng'$.*
3. *$\forall g \in G, gN = Ng$.*
4. *N is the kernel of a homomorphism.*
5. *N is the union of conjugacy classes.*

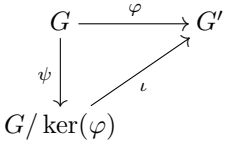
Proof. We already know that *1*, *2*, and *3*, and moreover, *4* $\implies$ *1* is clear, as is the equivalence of *5*. We will show *1* $\implies$ *4*.

Let $N \trianglelefteq G$, and define $\varphi : G \to G/N$ by $g \mapsto gN$. We claim that G/N is a group with the composition law $g_1N \cdot g_2N = g_1Ng_2N$. We note that $g_1(Ng_2)N = g_1g_2NN = g_1g_2N$. G/N has an identity $1N \in G/N$ and satisfies the inverse law $gN \cdot g^{-1}N = 1N$; it is associative by associativity of G and hence is a group. By our composition law, it is immediately clear that

$$\varphi(g_1g_2) = g_1g_2N = g_1N \cdot g_2N = \varphi(g_1)\varphi(g_2)$$

So φ is a homomorphism, and $N = \ker(\varphi)$. ■

Theorem 8.3 (First Isomorphism Theorem)**.** *Let $\varphi : G \to G'$ be a homomorphism of groups. We have by the previous theorem a homomorphism $\psi : G \to G/N$ for any $N \trianglelefteq G$. Then there is a unique injective homomorphism $\iota : G/\ker(\varphi) \to G'$ such that $\iota \circ \psi = \varphi$. Equivalently, we say that the following diagram is commutative:*



In particular, if φ is surjective, ι is an isomorphism.

Proof. Write $N = \ker(\varphi)$. Define ι by $\iota(gN) = \varphi(g)$. We must show that ι is a well-defined, injective homomorphism. Consider $g, g' \in N : gN = g'N$. Then $\exists n \in N : gn = g'1$. Hence, $\varphi(g') = \varphi(gn) = \varphi(g)\varphi(n) = \varphi(g)$, so ι is well-defined. We note also that ι is homomorphic because φ is homomorphic.

Let $g, g' \in G : \iota(gN) = \iota(g'N) \implies \varphi(g) = \varphi(g')$. $\exists x \in G : g' = gx$. Then $\varphi(g) = \varphi(gx) = \varphi(g)\varphi(x)$. So we must have $\varphi(x) = 1$, and so $x \in \ker(\varphi) \equiv N$. Then $g \in g'N$, so $gN = g'N$, and ι is injective. ■

Example.

$$\varphi : \mathbb{R}^+ \longrightarrow \mathbb{T}$$
$$x \longmapsto e^{2\pi i x}$$

$\ker(\varphi) = \mathbb{Z}^+$, so $\mathbb{R}^+/\mathbb{Z}^+ \cong \mathbb{T}$.

Example. $\mathbb{Z}^+ \twoheadrightarrow \mathbb{Z}^+/n\mathbb{Z}^+$

Example. Let $\mathbf{V}$ be the Klein four group. We can view $\mathbf{V} \leq S_4$ as a group of permutations

$$\{1, (12)(34), (13)(24), (14)(23)\}$$

We have shown previously that there is a surjective homomorphism $\varphi : S_4 \twoheadrightarrow S_3$. Based on our past construction, we see that $\mathbf{V} = \ker(\varphi)$. So $S_4/\mathbf{V} \cong S_3$.

Example. $\langle r \rangle \subset D_{2n}$, and $D_{2n}/\langle r \rangle$ is a group of order two.

Definition 8.4. We know there is a homomorphism

$$\det : GL_n(\mathbb{R}) \twoheadrightarrow \mathbb{R}^\times$$

Define the <u>special linear group</u> to be the subgroup

$$SL_n(\mathbb{R}) = \ker(\det)$$

Note that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$.

Definition 8.5. We also know there is an injective homomorphism

$$S_n \overset{i}{\hookrightarrow} GL_n(\mathbb{R}) \overset{\det}{\twoheadrightarrow} \mathbb{R}^\times$$

And we define the <u>sign</u> homomorphism

$$\operatorname{sgn} : S_n \to \{0, 1\}$$

by $\sigma \mapsto (-1)^n$, where n is the number of transpositions to which σ decomposes (the parity is invariant).

Definition 8.6. The <u>alternating group</u> $A_n \subset S_n$ is

1. $A_n = \ker(\operatorname{sgn})$
2. $A_n = \{\text{even permutations in } S_n\}$

Example. $S_3 \cong D_6$ $A_3 \cong \langle r \rangle$

Lecture 9 — 9/30/10

Remark. Recall the homomorphism $\varphi : G \twoheadrightarrow G/N$ with $\ker(\varphi) = N$. By the First Isomorphism Theory, G is "built-up" from N and G/N, $|G| = |N| \cdot |G/N|$.

Definition 9.1. A finite group G is called solvable if there is a sequence of groups

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_m = G$$

such that

1. $G_i \trianglelefteq G_{i+1}$.
2. $|G_{i+1}/G_i| = p_i$ prime; that is, G_{i+1}/G_i is cyclic of prime order.

Example. S_3 is solvable, as is S_4. The latter is solvable because $\varphi : S_4 \twoheadrightarrow S_3$, $\ker(\varphi) = \mathbf{V}$.

Definition 9.2. Let G_1, G_2 be groups. The product group is the set

$$G_1 \times G_2 = \{(g_1, g_2) : g_i \in G_i\}$$

with composition law defined by coordinates:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$$

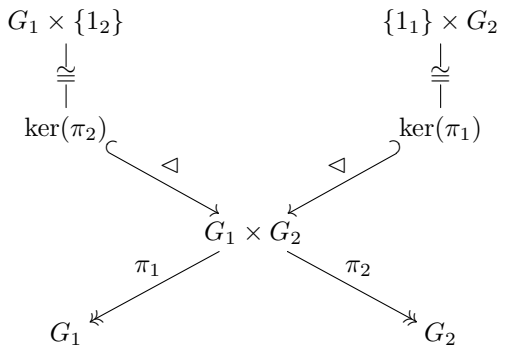
Claim 9.3. *$G_1 \times G_2$ is a group.*

Proof. $1_X = (1_1, 1_2)$ and $(g_1^{-1}, g_2^{-1}) = (g_1, g_2)^{-1}$. ∎

Note. $|G_1 \times G_2| = |G_1| \cdot |G_2|$

Example. $\mathbf{V} \cong C_2 \times C_2$

Observation 9.4. Consider the natural projection maps $\pi_i : G_1 \times G_2 \to G_i$. We have



By the First Isomorphism Theorem,

$$G_1 \times G_2 / G_1 \times \{1_2\} \cong G_2 \quad \text{and} \quad G_1 \times G_2 / \{1_1\} \times G_2 \cong G_1.$$

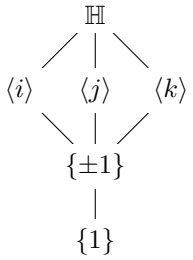
Theorem 9.5 (Fundamental Theorem of Abelian Groups)**.** *Let G be any finite abelian group. Then G is isomorphic to a finite product of cyclic groups. In particular, G is isomorphic to a finite product of cyclic groups of prime-power order.*

Definition 9.6. Define the quaternion group by

$$\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$$

where $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j$, and $(-1)^2 = 1$.

Observation 9.7. Let us explore $\mathbb{H}$. Consider its lattice of subgroups.



Note that every subgroup of $\mathbb{H}$ is normal, but $\mathbb{H}$ is non-abelian. Note also that $Z(\mathbb{H}) = \{\pm 1\}$. The only "interesting" quotient of $\mathbb{H}$ is $\mathbb{H}/Z(\mathbb{H}) \cong C_2 \times C_2 \cong \mathbf{V}$. Consider the automorphism group.

$$\mathrm{Aut}(\mathbb{H}) \ni \alpha \begin{cases} i \longmapsto \epsilon_i \cdot i' \\ j \longmapsto \epsilon_j \cdot j' \\ k \longmapsto \epsilon_k \cdot k' \end{cases}$$

where $\epsilon_i \in \{\pm 1\}, i', j', k' \in \{i, j, k\}$. We recognize a homomorphism

$$\ker(p) \hookrightarrow \mathrm{Aut}(\mathbb{H}) \xrightarrow{p} \twoheadrightarrow S_3$$

given by

$$\mathrm{Perm}\{i, j, k\} \cong S_3 \ni p(\alpha) = \begin{pmatrix} i & j & k \\ i' & j' & k' \end{pmatrix}$$

We also have a function giving us

$$\epsilon(\alpha) = (\epsilon_i, \epsilon_j, \epsilon_k) \in C_2 \times C_2 \times C_2$$

But not every triple $(\epsilon_i, \epsilon_j, \epsilon_k)$ yields an automorphism. For $\alpha \in \ker(p)$,

$$\alpha \longleftrightarrow \begin{cases} i \longmapsto e_i i \\ j \longmapsto e_j j \\ k \longmapsto e_k k \end{cases}$$

Since $ij = k$, we have $\alpha(i)\alpha(j) = \alpha(k)$, which means $\epsilon_i \epsilon_j ij = \epsilon_k k$. This yields a coherence condition

$$\epsilon_i \epsilon_j \epsilon_k = 1$$

or equivalently, a restriction to the kernel of a homomorphism

$$\ker(\gamma) \hookrightarrow C_2 \times C_2 \times C_2 \xrightarrow{\gamma} \twoheadrightarrow C_2$$

We note that $\ker(\gamma) \cong \ker(p) \cong \mathbf{V}$. So we have $\mathbf{V} \lhd \operatorname{Aut}(\mathbb{H})$ and $\operatorname{Aut}(\mathbb{H})/\mathbf{V} \cong S_3$, and hence

$$|\operatorname{Aut}(\mathbb{H})| = |\mathbf{V}| \cdot |S_3| = 4 \cdot 6 = 24$$

Lecture 10 — 10/5/10

Definition 10.1. A ring A is a set with two operations, $+$ and $\cdot$ such that

- A is an abelian group under $+$.
- $\cdot$ is associative.

The operations of $+$ and $\cdot$ are related by

- a two-sided distributive law.

A is a ring with unit if

- $\exists 1 : \forall x \in A, 1 \cdot x = x = x \cdot 1$.

We will use the term "ring" to mean "ring with unit."

Definition 10.2. A ring homomorphism $f : A \to A'$ is a map from a ring A to a ring A' such that

1. $f(a+b) = f(a) + f(b)$.
2. $f(a \cdot b) = f(a) \cdot f(b)$.
3. $f(1) = f(1')$.

Note that the third requirement is necessary to avoid categorizing, say, the zero map as a homomorphism.

Example.
1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings.
2. Let A be any commutative ring, let $n \geq 1$. Then $\operatorname{Mat}_n(A)$ is a ring.
3. Let A be any commutative ring. Then $A[X]$, is the polynomial ring in X with coefficients in A; it inherits commutativity from A. Likewise, $A[X_1, \ldots, X_n]$ is a polynomial ring.

Example. Let $f : A \to A'$ be a ring homomorphism between commutative rings A, A'. Then the map

$$\begin{aligned} f_n : M_n(A) &\longrightarrow M_n(A') \\ (a_{i,j}) &\longmapsto (f(a_{i,j})) \end{aligned}$$

is a ring homomorphism. Moreover, the map

$$\begin{aligned} \tilde{f} : A[X] &\longrightarrow A'[X] \\ \sum_{i=0}^{d} a_i X^i &\longmapsto \sum_{i=0}^{d} f(a_i) X^i \end{aligned}$$

is a ring homomorphism

Observation 10.3.

1. If
$$A \xrightarrow{f} A' \xrightarrow{g} A''$$
represent ring homomorphisms, then $gf : A \to A''$ is a ring homomorphism.
2. The zero map is only a ring homomorphism if the codomain is the zero ring.
3. There is exactly one ring homomorphism $\mathbb{Z} \to A$ for any ring A; it is entirely given by $f(n) = \underbrace{f(1) + \cdots + f(1)}_{n}$ and $f(-n) = -f(n)$.

Definition 10.4. Let A be a ring, $B \subseteq A$. B is a subring of A if B is a subgroup of $(A, +)$, is closed under multiplication, and contains the multiplicative identity. Note that B is also a ring.

Example. $\mathbb{R} \times \mathbb{R}$ is a commutative ring, as is $\mathbb{R} \times \{0\}$. However, $\mathbb{R} \times \{0\} \subset \mathbb{R} \times \mathbb{R}$ is not a subring.

Definition 10.5. Let $f : A \to A'$ be a ring homomorphism. The kernel of f is

$$\ker(f) = \{x \in A : f(x) = 0\}$$

Example. Let A be a commutative ring. Consider $A[X]$. Fix $a \in A$. The evaluation at a is the map

$$\begin{aligned} \operatorname{ev}_a : A[X] &\longrightarrow A \\ p(X) &\longmapsto p(a) \end{aligned}$$

ev_a is a ring homomorphism. Note that

$$\ker(\operatorname{ev}_a) = \{p(X) \in A[X] : a \text{ is a root}\}$$

Proposition 10.6. *$\forall x \in A$ a ring, $0 \cdot x = 0 = x \cdot 0$.*

Proof.

$$\begin{aligned} 0 + 0 &= 0 \\ (0+0)x &= 0x \\ 0x + 0x &= 0x \\ 0x &= 0 \end{aligned}$$

and right-multiplication by 0 is similar. ∎

Definition 10.7. Let A be a ring. A two-sided ideal in A is a subgroup $I \subseteq A$ (w.r.t. $(A, +)$) such that $\forall x \in A$,

$$x \cdot I \subseteq I \supseteq I \cdot x$$

Note that in a commutative ring, an ideal is necessarily two-sided.

Observation 10.8. Let $f : A \to A'$ be a ring homomorphism. Then $\ker(f)$ is an ideal.

Proof. Since f is a homomorphism of abelian groups, $\ker(f)$ is an abelian subgroup. We have that

$$f(xa) = f(x)f(a) = f(x) \cdot 0 = 0$$

so $xa \in \ker(f)$; the proof for ax is similar. ■

Claim 10.9. *The intersection of any number of two-sided ideals is again a two-sided ideal.*

Definition 10.10. Let A be a commutative ring, $a \in A, S \subseteq A$. The ideal generated by a is the intersection of all ideals in A containing a. Equivalently, it is

$$(a) := aA = \{a \cdot b : b \in A\}$$

The ideal generated by S is the intersection of all ideals in A containing S, or alternatively,

$$(S) := \sum_{s \in S} sA$$

Definition 10.11. A principal ideal is an ideal generated by a single element.

Theorem 10.12. *Any ideal in $\mathbb{Z}$ is principal.*

Proof. This follows from the fact that every subgroup of $\mathbb{Z}$ is generated by a single element. ■

Theorem 10.13 (Unique Factorization Theorem)**.**

Example. Consider the ring $A = \{a + b\sqrt{6} : a, b \in \mathbb{Z}\}$. Factorizations are not unique in A ($6 = \sqrt{6} \cdot \sqrt{6} = 2 \cdot 3$). Moreover, note that A is "missing" $\gcd(\sqrt{6}, 2) = \sqrt{2}$ and $\gcd(\sqrt{6}, 3) = \sqrt{3}$. However, we do have the ideals $(\sqrt{6}, 2)$ and $(\sqrt{6}, 3)$; they are "ideal elements" of A.

Lecture 11 — 10/11/10

Definition 11.1. Let A be a ring. The group of units of A is the set

$$A^* = \{x \in A : \exists x^{-1}, x \cdot x^{-1} = 1 = x^{-1} \cdot x\} \subseteq A$$

Note that $1 \in A^*$ and that A^* is closed under multiplication, so A^* is indeed a group.

Example.

1. Consider the matrix ring $M_n(A)$ where A is a commutative ring. We have $M_n(A)^* = GL_n(A)$.
2. Let $A \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Then $A^* = A - \{0\}$.
3. $\mathbb{Z}^* = \{\pm 1\}$.
4. Consider the polynomial ring $A[X]$. $A[X]^* = A^*$.

Definition 11.2. A field is a commutative ring F such that $F^* = F - \{0\}$ and $0 \neq 1$.

Theorem 11.3. *Let A be a ring, $I \subseteq A$ a subset. I is the kernel of a ring homomorphism iff it is a two-sided ideal.*

Proof. Let

$$I \subseteq A \xrightarrow{f} A'$$

where $I = \ker f = \{a \in A : f(a) = 0\}$. Then I is a normal abelian group under $+$, and is closed under left and right multiplication; it is a two-sided ideal.

Conversely, let $I \subseteq A$ be a two-sided ideal. Consider A/I, a quotient of abelian groups under addition. Then we have a natural group homomorphism

$$A \xrightarrow{f} A/I$$

such that $\ker f = I$. It remains to be shown that we can make A/I a ring which makes f into a ring homomorphism with kernel I. We know that an element $a \in A/I$ is a coset of the form $\overline{a} + I$. Consider another coset $\overline{b} + I$. If we want f to be a ring homomorphism, we must require

$$f(a \cdot b) = \overline{a} \cdot \overline{b} + I = (\overline{a} + I) \cdot (\overline{b} + I) = f(a) \cdot f(b)$$

This yields a definition of multiplication in A/I

$$(\overline{a} + I) \cdot (\overline{b} + I) = \overline{a} \cdot \overline{b} + I$$

We must show that this operation is well-defined. Let $\overline{a} + I = \overline{\alpha} + I$ and $\overline{b} + I = \overline{\beta} + I$. Then $\exists i_1, i_2 \in I$: $\overline{\alpha} = \overline{a} + i_1, \overline{\beta} = \overline{b} + i_2$. This yields

$$\overline{\alpha}\overline{\beta} = \overline{a}\overline{b} + (\overline{a}i_2 + i_1\overline{b} + i_1 i_2)$$

But $\overline{a}i_2 + i_1\overline{b} + i_1 i_2 \in I$ since I is a two-sided ideal. So

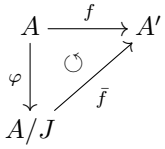
$$(\overline{\alpha} + I) \cdot (\overline{\beta} + I) = \overline{\alpha}\overline{\beta} + I = \overline{a}\overline{b} + I = (\overline{a} + I) \cdot (\overline{b} + I)$$

as desired. ■

Definition 11.4. Let $I \subseteq A$ be an ideal of a commutative ring. By Theorem 11.3, there is a ring structure on A/I, termed the quotient ring.

Note. Every ring A has at least two two-sided ideals, the zero ideal $(0) = \{0\}$ and the unit ideal A. In particular, $A = (u)$ for any $u \in A^*$. Moreover, note that $A/(0) = A$ and $A/(1) = \{0\}$. An ideal that is not the unit ideal or the zero ideal is called a proper ideal.

Theorem 11.5 (First Isomorphism Theorem)**.** *Let $f : A \to A'$ be a ring homomorphism, and write $I = \ker(f)$. Let $J \subseteq I$ be an ideal. We have by the previous theorem a homomorphism $\varphi : A \to A/J$. Then there is a unique homomorphism $\bar{f} : A/J \to A'$ such that $\bar{f} \circ \varphi = f$.*



and if $J = I$ and f is surjective, then $\bar{f}$ is an isomorphism yielding $A/\ker(f) \cong A'$.

Definition 11.6. An integral domain is a commutative ring A where $c, d \in A : c \cdot d = 0 \implies c = 0$ or $d = 0$. Equivalently, we say A satisfies a cancellation law, wherein $a, b, c \in A : c \neq 0, c \cdot a = c \cdot b \implies a = b$.

Definition 11.7. Let A be a ring, $d \in A$. We call d a zero divisor if $\exists c \neq 0 : cd = 0$ (in this case, d is a right zero divisor). Note that an integral domain is a commutative ring with no zero divisors.

Definition 11.8. A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Example. Let $S = \{a, b : a, b \neq 0\} \subseteq \mathbb{Z}$. Then we can write

$$\begin{aligned}(S) &= \{ar + bs : r, s \in \mathbb{Z}\} \\ &= \gcd(a, b) \cdot \mathbb{Z}\end{aligned}$$

So $\mathbb{Z}$ is a PID.

Note. If A is commutative, $S = \{a_1, \ldots, a_n\} \subseteq A$, then $(S) = \{\sum_{i=1}^n r_i a_i : r_i \in A\}$.

Example. Any field F is a principal ideal domain, since each field has only the zero ideal and the unit ideal by definition, both of which are principal.

Definition 11.9. Let A be a PID, $a, b \in A$. Suppose that $(a) = (b)$. Then $a \cdot A = b \cdot A$, so $a = b \cdot m, b = a \cdot n$ for some $m, n \in A$. So $a = a \cdot n \cdot m$, which yields, by cancellation, $1 = n \cdot m \iff n = m^{-1}$. This means that n and m are units and yields an equivalence relation $a \sim b$ iff $a = u \cdot b$ where $u \in A^*$. We call this relation association, and we note that this partitions A into associate classes of A, which we denote $a \cdot A^*$.

Example. Let $A = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Then A is closed under multiplication

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}$$

and A is a field, since $(a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2 \neq 0$, and

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2}$$

Claim 11.10. *Consider the integral domain $\mathbb{Q}[X]$ and the ideal $(X^2-2) = (X^2-2)\mathbb{Q}[X]$. Then $\mathbb{Q}[X]/(X^2-2) = \mathbb{Q}[\sqrt{2}]$.*

Proof. Recall the evaluation homomorphism, which here is surjective

$$\begin{aligned}\text{ev} : \mathbb{Q}[X] &\twoheadrightarrow \mathbb{Q}[\sqrt{2}] \\ X &\longmapsto \sqrt{2}\end{aligned}$$

We have

$$\ker \text{ev} = \{f(X) \in \mathbb{Q}[X] : f(\sqrt{2}) = 0\}$$

So for any polynomial $\sum_{n=0}^d a_n X^n$, we must have $\sqrt{2}$ as a root.

$$\sum_{n=0}^{d} a_n (\sqrt{2})^n = \sum_m a_{2m} 2^m + \sum_m a_{2m+1} 2^m \sqrt{2} = 0$$

So if $\sqrt{2}$ is a root, then $-\sqrt{2}$ is also a root. So $(X^2 - 2) | f(X)$. By the First Isomorphism Theorem, we get $\mathbb{Q}[X]/\ker \text{ev} \cong \mathbb{Q}[\sqrt{2}]$. ■

Lecture 12 — 10/14/10

Definition 12.1. A ring A' that contains A as a subring is a ring extension of A. The adjunction of a new element α to a ring A is

$$A[\alpha] = \left\{ \sum_{i=0}^{n} r_i \alpha^i : n \in \mathbb{N}, r_i \in A \right\}$$

This is the image of the "evaluation" of $R[X]$ at α.

Remark. Begin with a commutative ring, say $\mathbb{Q}$. Suppose we want to construct a ring containing elements satisfying a given relation, say $X^{100} = 0, X^{99} \neq 0$. Adjoin an unknown (a variable) X to form a polynomial ring, $\mathbb{Q}[X]$, and then quotient by the desired relation.

$$\begin{aligned}\varphi : \mathbb{Q}[X] &\twoheadrightarrow \mathbb{Q}[X]/(X^{100}) \\ X &\longmapsto \theta \\ X^{100} &\longmapsto \theta^{100} = 0\end{aligned}$$

We have

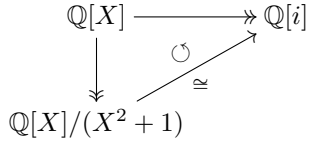
$$\ker(\varphi) = (X^{100}) = \{X^{100} \cdot P(X) : P(X) \in \mathbb{Q}[X]\}$$

Note that $X^{99} \neq X^{100} P(X)$, so this condition is always satisfied.

If, on the other hand, we want to impose a relation $a = 0$ on a ring A for some $a \in A$, we take the quotient ring $A/(a)$, the elements of which are $\overline{b} = b + (a)$, to which every element $b + ar$ is mapped (for some fixed $b \in A$ and any $r \in A$). Note also that if $uv + w = a$ for $u, v, w \in A$, then

$$\overline{uv} + \overline{w} = \overline{uv + w} = \overline{a} = 0$$

Definition 12.2. Consider the diagram



which is commutative by the First Isomorphism Theorem. The Gaussian numbers are the ring

$$\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$$

And the Gaussian integers are the ring

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

Note that

$$\mathbb{R}[i] \cong \mathbb{C}$$

Example. Consider the diagram

$$\begin{array}{ccc} \mathbb{Q}[X,Y] & \twoheadrightarrow & \mathbb{Q}[\sqrt{2},\sqrt{3}] \\ {\scriptstyle h}\downarrow & \circlearrowleft & \nearrow{\scriptstyle \cong} \\ \mathbb{Q}[X,Y]/(X^2-2, Y^2-3) & & \end{array}$$

where we have

$$\begin{aligned} \ker(h) &= (X^2-2, Y^2-3) \\ &= \{(X^2-2)P(X) + (Y^2-3)Q(X)\} \end{aligned}$$

and $h(X) = \theta_2, h(Y) = \theta_3$. Then $h(X^2-2) = 0 \implies \theta_2^2 - 2 = 0$ and $h(Y^2-3) = 0 \implies \theta_3^2 - 3 = 0$.

Example. Suppose we want to give $2 \in \mathbb{Z}$ an inverse; that is, we want $X : 2X - 1 = 0$. Take the quotient

$$\mathbb{Z}[X]/(2X-1) \cong \mathbb{Z}[\frac{1}{2}]$$

which is the smallest subring of $\mathbb{Q}$ containing $\frac{1}{2}$.

Example. In general, if $a \in A$ a commutative ring, we can "invert" a by taking

$$\begin{aligned} A[X] &\twoheadrightarrow A[X]/(aX-1) \\ x &\longmapsto a^{-1} \end{aligned}$$

Note that if $a = 0$, we get

$$A[X]/(-1) = A[X]/A[X] = (0)$$

Definition 12.3. A monoid is a set with an associative composition law and an identity, but not necessarily having inverses.

Example. $\mathbb{Q}[i]$ is a field. Consider the ring homomorphism $N : \mathbb{Q}[i] - \{0\} \longrightarrow \mathbb{Q}^{>0}$

$$N(a+bi) := \|a+bi\| = (a+bi)(a-bi) = a^2 + b^2$$

which is called the norm. We also have a similar map $N : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{Z}^{>0}$; in this case, N is a monoid homomorphism with respect to multiplication. Elements of $\mathbb{Q}[i] - \{0\}$ are invertible

$$(a+bi)^{-1} = \frac{1}{a+bi} = \frac{a}{N(a+bi)} - \frac{b}{N(a+bi)}i$$

and both $\mathbb{Z}[i]$ and $\mathbb{Q}[i]$ are integral domains; they are subrings of fields, and all fields are integral domains.

Proposition 12.4. *$\mathbb{Z}[i]$ is a principal ideal domain.*

Proof. Let $I \subset \mathbb{Z}[i]$. We want to find $\gamma \in \mathbb{Z}[i]$ such that

$$I = (\gamma) = \gamma \cdot \mathbb{Z}[i]$$

We will follow the proof that $\mathbb{Z}$ is a PID. Let $J \subset \mathbb{Z}$ be a nonzero ideal, $a \in J$. Then $|a| \in \mathbb{Z}^{>0}$, and recall that the norm N is a homomorphism with respect to multiplication. Find a nonzero element $a \in J$ of smallest norm. Now take any $b \in J$. We want to show that $a \,|\, b$. We can write $b = ma + r, 0 \le |r| < |a|$. Then $r = b - ma \in J$. If $r \neq 0$, then a was not minimal. $\Rightarrow\Leftarrow$. Note also that

$$\frac{b}{a} = \frac{ma}{a} + \frac{r}{a} = m + \frac{r}{a}$$

which is to say that any rational can be written as an integer plus a rational of norm < 1.

Now let us prove the claim for the Gaussian integers. Geometrically, we see that $\forall g \in \mathbb{Q}[i], \exists m \in \mathbb{Z}[i] : g - m \in \mathbb{Q}[i]$ has norm $N(g-m) < 1$. We can choose $g = a + bi$, and $m = a' + b'i$, and $|a' - a| \le \frac{1}{2}, |b' - b| \le \frac{1}{2}$.

Let $I \neq (0)$ be an ideal in $\mathbb{Z}[i]$ and let $\gamma = a + bi \in I$ of smallest norm $N(\gamma) = a^2 + b^2$. Let $\eta \in I$; we want to show that $\gamma \,|\, \eta$. Let $g = \frac{\eta}{\gamma}$. We know $g = m + r$, $m \in \mathbb{Z}[i]$, $r \in \mathbb{Q}[i] : N(r) < 1$. Multiplying by γ, we get

$$\gamma g = \eta = \gamma m + \gamma r$$

Note that $N(\gamma r) = N(\gamma)N(r) < N(\gamma)$. But we have $\gamma r = \eta - \gamma m \in I$, in which γ was chosen to have minimal norm. $\Rightarrow\Leftarrow$. So $\eta \,|\, \gamma$, and hence $\mathbb{Z}[i]$ is a principal ideal. ■

Proposition 12.5. *If $a \,|\, n$, then the map $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/a\mathbb{Z}$ given by $\overline{x}_n \mapsto \overline{x}_a$ is a ring homomorphism.*

Theorem 12.6 (Chinese Remainder Theorem)**.** *Let $a, b \in \mathbb{Z}$ such that $\gcd(a,b) = 1$ (that is, a and b are coprime). Write $n = ab$. Then $\exists s, t \in \mathbb{Z} : 1 = sa + tb$. Then the map*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \overline{x}_n &\longmapsto (\overline{x}_a, \overline{x}_b) \end{aligned}$$

is a ring homomorphism. Moreover, it is an isomorphism, and its inverse is given by $(\overline{u}_a, \overline{v}_b) \mapsto \overline{sav + tbu}_n$.

Lecture 13 — 10/19/10

Theorem 13.1 (Correspondence Theorem)**.** *Recall the canonical map*

$$\varphi : A \twoheadrightarrow A/I$$

for an ideal $I \subseteq A$ a ring. Let $\overline{A} = A/I$. Then there is a bijection

$$\{J \subseteq A : J \supseteq I\} \longleftrightarrow \{\overline{J} \subseteq \overline{A}\}$$

where J and $\overline{J}$ are ideals of A and $\overline{A}$ respectively; that is to say, a bijection between ideals in A containing I and ideals in $\overline{A}$. This bijection is given by

$$J \longmapsto \varphi(J) \qquad \overline{J} \longmapsto \varphi^{-1}(\overline{J})$$

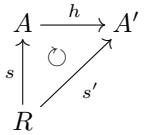
Note. $\overline{J}$ is a collection of I-cosets of A, and J is the union of the I-cosets in $\overline{J}$, where $J \leftrightarrow \overline{J}$. Note also that $I \subseteq J$, $I \leftrightarrow \{0\}$, and $\{0\} \subseteq \overline{J}$.

Proof. ■

Let $f : R \twoheadrightarrow R'$ be a surjective ring homomorphism. Then the ideals in R containing $\ker f$ and the ideals in R' biject by the First Isomorphism Theorem. $R \to R/I$, $R/I \cong R'$, $f : R \twoheadrightarrow R'$.

Definition 13.2. Let R be a ground ring, and consider rings A that are equipped with a ring homomorphism $s : R \to A$. The pair (A, s) is called a R-algebra. With s, called the structure homomorphism, understood, we say that A is an R-algebra.

Definition 13.3. An R-algebra homomorphism is a ring homomorphism $h : A \to A'$ between R-algebras that makes the following diagram commutative.



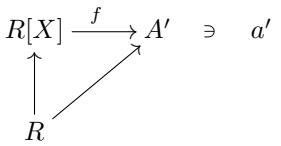
which is to say that h preserves the structure homomorphisms.

Example. A structure homomorphism is not, in general, unique. However, there is exactly one homomorphism $\mathbb{Z} \to A$ for any ring A, so every ring A is a $\mathbb{Z}$-algebra, with a uniquely determined structure.

Example. $R = \mathbb{C}$, $(z + 0x + \cdots)\mathbb{C}[X]$

Definition 13.4. Let A be an R-algebra, $a \in A$. The couple (A, a) has the free property if for every couple (A', a'), an R-algebra and an element, there is a unique R-algebra homomorphism $A \to A'$ given by $a \mapsto a'$. The free property is a universal property.

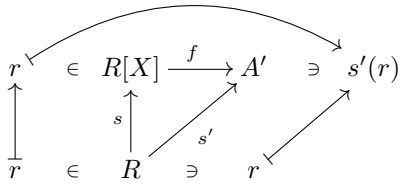
Observation 13.5. Consider $(A, a) = (R[X], X)$. We want to find a unique R-algebra homomorphism f that makes the following diagram commutative:



Define f by

$$f\left(\sum_{i=0}^{d} r_i X^i\right) = \sum_{i=0}^{d} s'(r_i)(a')^i \in A'$$

f is the unique R-algebra homomorphism sending $X \mapsto a'$.



The freeness property completely characterizes $(R[X], x)$; it is the unique R-algebra such that $(R[X], x)$ satisfies freeness.

Proposition 13.6. *Suppose that A_1, A_2 are R-algebras such that (A_1, a_1) and (A_2, a_2) both satisfy freeness. Then there exists a unique R-algebra homomorphism $A_1 \to A_2$ given by $a_1 \mapsto a_2$, and this homomorphism is an isomorphism.*

Proof. Considering each (A_i, a_i) with the free property in turn, and the other (A_j, a_j) as an arbitrary couple for which the free property must be satisfied, we get unique functions f, g as follows:

$$\begin{array}{ccc} A_1 \xrightarrow{f} A_2 & \qquad & A_1 \xleftarrow{g} A_2 \\ a_1 \longmapsto a_2 & & a_1 \longmapsfrom a_2 \end{array}$$

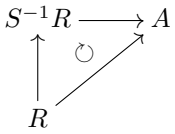
Then taking (A_i, a_i) as both the the couple satisfying the free property and the arbitrary couple for with the property is satisfied, we find that the identity homomorphisms $A_1 \to A_1$ and $A_2 \to A_2$ are unique. So $f \circ g \equiv \mathrm{id}_2$ and $g \circ f \equiv \mathrm{id}_1$. ■

Remark. Thus, the polynomial ring $R[X]$ is characterized as the unique R-algebra such that $(R[X], X)$ satisfies freeness.

Observation 13.7. Now let R be a commutative ring, $S \subseteq R$ a subset. Consider the collection of R-algebras A such that the image of S under the structure homomorphism is invertible. We want to find a universal object in this collection; that is, we want an R-algebra $S^{-1}R$ such that

1. The image under the structure homomorphism $s : R \to S^{-1}R$ is invertible.

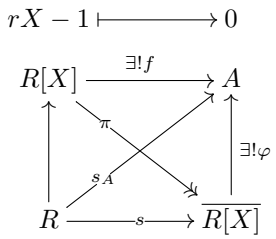
2. For every R-algebra A in the collection given by the above property, there is a unique R-algebra homomorphism such that the following diagram commutes:



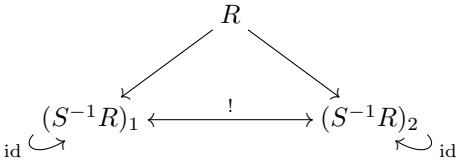
Example. Let $S = \{r\} \subseteq R$; let us invert r. Take

$$S^{-1}R = R[X]/(rX - 1) =: \overline{R[X]}$$

If A is in our collection, then we have



where f is given by the freeness property described above, and φ is given by the First Isomorphism Theorem. The same method as with polynomial rings shows that $S^{-1}R$ satisfying the property of being a universal object in our collection uniquely characterizes it.



Observation 13.8. Does $S^{-1}R$ always exist? We have shown that it does if $|S| = 1$. If $S = \{r_1, r_2, \ldots, r_n\}$ is finite, inverting S is equivalent to inverting the product $r_1 r_2 \cdots r_n$.

For arbitrary S, we can still find $S^{-1}R$. Take the polynomial ring

$$R[x_\sigma : \sigma \in S]/I$$

where $I = (x_\sigma - 1 : \sigma \in S)$.

Example. Let $R = \mathbb{Z}, S = \mathbb{Z} - \{0\}$. Then $S^{-1}R = \mathbb{Q}$.

Lecture 14 — 10/21/10

Remark. Let $S \subseteq A$ be a subset of a commutative ring with unit. Recall that $S^{-1}A$ is an A-algebra which is the universal solution to the problem of inverting the elements of S. Let us determine the kernel of the A-algebra homomorphism

$$A \longrightarrow S^{-1}A$$

Let us first consider the case where S is a monoid.

Example. Let $S = A - \{0\}$, $1 \neq 0$. We know that $1 \in S$. It is clear that S is a monoid iff A is an integral domain; that is to say, if and only if A has no zero divisors.

Proposition 14.1. *Let $S_0 \subseteq A$ any subset. Let*

$$S = \{s_1 \cdots s_n : s_i \in S_0\}$$

be the monoid generated by S_0. Then $S_0^{-1}A \cong S^{-1}A$.

Proof. This is clear; inverting individual elements yields an inverse for their product, and inverting the product yields inverses for the individual elements by uniqueness. ■

Theorem 14.2. *Let $S \subseteq A$ a commutative ring. Denote the canonical map to $S^{-1}A$ by $\varphi : A \to S^{-1}A$. Then*

$$\ker(\varphi) = \left\{a \in A : \exists s_i \in S^{-1}, \prod s_i \cdot a = 0\right\}$$

Proof. We will prove the theorem for the case where S is finite. By the above proposition, we may equivalently prove the case for $S = \{s\}$. We want to show that

$$\ker(\varphi) = \{a \in A : \exists n \geq 0, s^n a = 0\}$$

Recall the construction $S^{-1}A = A[X]/(sX - 1)$. We have

$$\begin{array}{ccc} A[X]/(sX-1) & = & S^{-1}A \\ \uparrow\!\uparrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \varphi} \\ A[X] & \longleftarrow & A \end{array}$$

Thus we have a map $\ker(\varphi) \to \ker(\pi) = (sX - 1)$. Choose $a \in \ker(\varphi)$. Then $a \mapsto (sX - 1)p(X)$ for some $p(X) \in A[X]$, where $(sX-1)p(X)$ is some constant polynomial a_0. Let us write

$$p(X) = c_0 + c_1 x + \cdots + c_d x^d$$

So we have

$$\begin{aligned} a_0 &= c_0 sx + c_1 sx^2 + \cdots + c_d sx^{d+1} - c_0 - c_1 x - \cdots - c_d x^d \\ &= -c_0 + (c_0 s - c_1)x + \cdots + (c_{d-1}s - c_d)x^d + c_d s x^{d+1} \end{aligned}$$

This yields

$$\begin{aligned} c_0 &= -a_0 \\ c_1 &= sc_0 = -sa_0 \\ c_2 &= sc_1 = -s^2 a_0 \\ &\vdots \\ c_d &= sc_{d-1} = -s^d a_0 \\ 0 &= sc_d = -s^{d+1} a_0 \end{aligned}$$

Hence, we have $s^{d+1}a = 0$, so

$$\ker(\varphi) \subseteq \{a \in A : \exists n \geq 0, s^n a = 0\}$$

The other inclusion is clear; this completes the proof. ■

Definition 14.3. Recall that $A - \{0\}$ is a monoid iff A is an integral domain. Then the map $\varphi : A \to S^{-1}A$ has $\ker(\varphi) = 0$, and from these two facts it is clear that $S^{-1}A$ is a field. $S^{-1}A$ is called the fractional field of the integral domain A.

Definition 14.4. Let R be a commutative ring with unit. An R-module M is an abelian group under $+$ together with a scalar multiplication operation $\cdot$ by R defined by

$$\begin{aligned} R \times M &\longrightarrow M \\ (r, m) &\longmapsto r \cdot m \end{aligned}$$

with

1. identity: $1 \cdot m = m$;
2. associativity: $r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \cdot m$; and
3. distributivity: $r \cdot (m + m') = rm + rm'$
   $(r + r') \cdot m = rm + r'm$

Example. A $\mathbb{Z}$-module grants no extra structure; any abelian group M is a $\mathbb{Z}$-module, since $1 \cdot m = m$, which determines $n \cdot m$.

Example. If A is an R-algebra, it is also an R-module by its own multiplication.

Definition 14.5. An R-module homomorphism is a map $f : M \to M'$ between R-modules such that

1. f is an abelian group homomorphism.
2. f is homogenous with respect to scalar multiplication; that is, $\forall r \in R, m \in M, f(r \cdot m) = r \cdot f(m)$.

Example. Let R be a ring. Define

$$R^n = \underbrace{R \times \cdots \times R}_{n}$$

R^n is an R-module with addition and scalar multiplication as in vector spaces. Consider the set $\{\epsilon_i\}_{i=1}^n$ given by

$$\epsilon_i = (\underbrace{0, \ldots, 1}_{i}, \ldots, 0)$$

This set generates R^n as an R-module; that is, any $m \in R^n$ is a linear combination of $\{\epsilon_i\}_{i=1}^n$; that is,

$$m = \sum r_i \epsilon_i$$

Definition 14.6. An R-module M is a free module if it has a free basis, that is, a linearly independent finite generating set $\{\epsilon_i\}_{i=1}^n$. Equivalently, given any other R-module N and set of elements $y_i \in N$, there exists a unique R-module homomorphism

$$\begin{aligned} M &\longrightarrow N \\ \epsilon_i &\longmapsto y_i \end{aligned}$$

Proposition 14.7. *R^n is a free module.*

Proof. Write $m = \sum r_i \epsilon_i \in R^n$. Define $f : R^n \to N$ by $f(\epsilon_i) = y_i$. This forces

$$f(m) = f\left(\sum r_i \epsilon_i\right) = \sum r_i f(\epsilon_i) = \sum r_i y_i$$

since f is defined to be a homomorphism. Consider any $m' = \sum r_i' \epsilon_i$. f is well-defined since $m = m' \iff r_i = r_i'$ for every i, and it is clearly unique. We should show in more detail that f is an R-module homomorphism, but we will not. ■

Definition 14.8. Let A be a ring. A maximal ideal is a proper ideal $I \subseteq A$ such that $\nexists J \subseteq A$ an ideal such that

$$I \subsetneq J \subsetneq A$$

Proposition 14.9. *Let A be a ring. An ideal $I \subseteq A$ is maximal iff A/I is a field.*

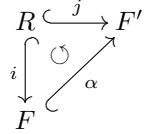
Proof. A/I is a field iff the only ideals of A/I are (0) and (1). The result is an easy consequence of the Correspondence Theorem. ■

Lecture 15 — 10/26/10

Remark. Let R be a ring, $S \subseteq R$ a monoid. Recall that $S^{-1}R$ is the unique R-algebra with structure homomorphism $i : R \to S^{-1}R$ such that $i(S)$ is invertible. Writing $i(x) = \overline{x}$, we have

$$i(S) = \{\overline{s}^{-1}\overline{a} : s \in S, a \in R\} \subseteq S^{-1}R$$

Theorem 15.1. *Let $R \hookrightarrow F'$ be an imbedding of R as a subring in a field F'. Let F be the field of fractions of R. Then there is a unique injective homomorphism $\alpha : F \to F'$ making the following diagram commutative:*



Proof. We define α by

$$\frac{a}{s} \longmapsto \frac{j(a)}{j(s)}$$

The result is clear. ■

Definition 15.2. Let A be a ring. A prime ideal is an ideal $I \subseteq A$ such that $\forall x, y \in A$, if $x \cdot y \in I$, then either $x \in I$ or $y \in I$.

Proposition 15.3. *Let A be a ring. An ideal $I \subseteq A$ is prime iff A/I is an integral domain.*

Proof. Suppose that I is prime, and let $\varphi : A \to A/I$ denote our canonical map into the quotient ring. We will denote $\varphi(x) = \overline{x}$ for any $x \in A$. Choose $\overline{x}, \overline{y} \in A/I$ such that $\overline{xy} = 0$. Then we have $xy \in \ker(\varphi) = I$. By primality, either $x \in \ker(\varphi)$ or $y \in \ker(\varphi)$. Thus, either $\overline{x} = 0$ or $\overline{y} = 0$. The proof in the other direction is analogous. ■

Example. In $\mathbb{Z}$, the maximal ideals are precisely those ideals generated by prime numbers $p \in \mathbb{P}$

$$(2), (3), (5), (7), (11), \dots$$

The prime ideals are the same, along with (0), since $\mathbb{Z}$ is an integral domain.

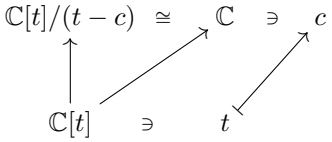
Example. Consider $\mathbb{C}[t]$. The Fundamental Theorem of Algebra states that $\mathbb{C}$ is algebraically closed; that is, every nonconstant polynomial in $\mathbb{C}[t]$ has a root. It follows that any monic polynomial $p(t)$ of degree $d > 0$ can be written

$$p(t) = (t - c_1)(t - c_2) \cdots (t - c_d)$$

Then it is clear that the maximal ideals of $\mathbb{C}[t]$ are

$$(t - c), \forall c \in \mathbb{C}$$

These, along with (0), are also the prime ideals. Note that



So the maximal ideals of $\mathbb{C}[t]$ correspond bijectively to $\mathbb{C} - \{0\}$. The group of units of $\mathbb{C}[t]$ is also

$$\mathbb{C}[t]^* = \mathbb{C}^* = \mathbb{C} - \{0\}$$

Moreover, $\mathbb{C}[t]$ is a PID, as well as a unique factorization domain, where every polynomial can be factored into irreducible polynomials $(t - c), c \in \mathbb{C}$ and some unit $c^* \in \mathbb{C}[t]^*$.

Observation 15.4. Let F be any field, and consider $F[t]$. The group of units $F[t]^* = F^*$ and the maximal ideals are the monic irreducible polynomials in $F[t]$.

Example. Let $F = \mathbb{R}$. What are the irreducible polynomials in $\mathbb{R}$?

$$p(t) = \prod_{i=1}^{d}(t - c_i) = \prod_{i=1}^{d_1}(t - r_i) \cdot \prod_{j=1}^{d_2}[(t - c_j)(t - \overline{c_j})]$$

where $d = d_1 + d_2$ and r_i are all the $c_i \in \mathbb{R}$. The maximal ideals in $\mathbb{R}[t]$ are those generated by $(t - r)$ or by $(t - c)(t - \overline{c})$.

Example. Let $\mathbb{C}$ and consider the $\mathbb{C}$-algebra

$$R := \mathcal{C}([0, 1], \mathbb{C})$$

There is a natural $\mathbb{C}$-algebra homomorphism, the evaluation at x, given by

$$\begin{aligned} \mathrm{ev}_x : R &\longrightarrow \mathbb{C} \\ f(t) &\longmapsto f(x) \end{aligned}$$

The kernel of the evaluation map is given by

$$I_x := \ker(\mathrm{ev}_x) = \{f(t) \in R : f(x) = 0\}$$

Note that $\forall f \in R, f - f(x) \in I_x \iff f \in f(x) + I_x$, and hence $R/I_x \cong \mathbb{C}$. Thus, I_x is maximal. Since ev_x is surjective, we have a map from $[0, 1]$ to the maximal ideals in R given by $x \mapsto I_x$.

Example. Consider $\mathbb{C}[x, y]$, the polynomial ring in two variables over the complex numbers. The maximal ideals in $\mathbb{C}[x, y]$ are not principal, but the prime ideals, which are the maximal ideals along with the zero ideal, are principal. For any pair $(a, b) \in \mathbb{C} \times \mathbb{C}$, consider the ideal

$$(x - a, y - b) \subseteq \mathbb{C}[x, y]$$

Consider the evaluation homomorphism at a, b,

$$\mathrm{ev}_{a,b} : \mathbb{C}[x, y] \to \mathbb{C}$$

we know that $x - a, y - b \in \ker(\mathrm{ev}_{a,b})$, and hence also $(x - a, y - b) \subseteq \ker(\mathrm{ev}_{a,b})$. Consider $p(x, y) \in \ker(\mathrm{ev}_{a,b})$. We can write

$$p(x, y) = p_{0,0} + p_{1,0}x + p_{0,1}y + p_{1,1}xy + \cdots$$

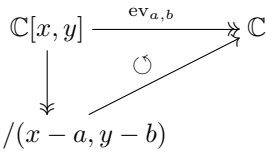
Substituting $x = a + x'$ and $y = b + y'$, expanding, and then back-substituting $x' = x - a$ and $y' = y - b$, we get

$$\begin{aligned} p(x, y) = p(a, b) &+ c_a(x - a) + c_b(y - b) + c_{aa}(x - a)^2 \\ &+ c_{ab}(x - a)(x - b) + c_{ba}(x - b)(x - a) \\ &+ c_{bb}(x - b)^2 + \cdots \end{aligned}$$

which coincides with the Taylor expansion of $p(x, y)$. Since $p(x, y) \in \ker(\mathrm{ev}_{a,b})$, $p(a, b) = 0$. Hence,

$$(x - a, y - b) = \ker(\mathrm{ev}_{a,b})$$

which means that



Hence, $\mathbb{C}[X, Y]/(x - a, y - b) \cong \mathbb{C}$, so $(x - a, y - b)$ is maximal.

Example. The ideal $(y - x^2)$ is the set of polynomials in the plane that vanish on the parabola $y = x^2$.

Theorem 15.5 (Hilbert's Nullstellensatz)**.** *All maximal ideals in $\mathbb{C}[x_1, \dots, x_n]$ are of the form*

$$(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$$

and hence are in bijection with elements of $\mathbb{C}^n$.

Lecture 16 — 10/28/10

Theorem 16.1 (Hilbert's Nullstellensatz)**.** *The maximum spectrum of $\mathbb{C}[x_1, \dots, x_n]$ is in bijection with $\mathbb{C}^n$, given by $(a_1, \dots, a_n) \longleftrightarrow (x_1 - a_1, \dots, x_n - a_n)$.*

Proof. By a proof analogous to that given in the example from last lecture, we know that every ideal of the form $(x_1 - a_1, \dots, x_n - a_n)$ is maximal. Now let $M \subseteq \mathbb{C}[x_1, \dots, x_n]$ be any maximal ideal. Write

$$K = \mathbb{C}[x_1, \dots, x_n]/M$$

and denote the canonical map into the quotient ring by

$$\varphi : \mathbb{C}[x_1, \dots, x_n] \to K$$

We will consider K to be a $\mathbb{C}$-algebra, a field extension, a quotient, and a vector space over $\mathbb{C}$. Consider the restriction of φ to the subring $\mathbb{C}[x_i]$,

$$\varphi_i : \mathbb{C}[x_i] \to K$$

Suppose that $\ker \varphi_i \neq (0)$. Let $p \in \ker \varphi_i$, $p \neq 0$. Since K is not the zero ring, $\ker \varphi_i \neq \mathbb{C}[x_i]$. Then p is nonconstant, so $\exists a_i \in \mathbb{C} : x_i - a_i \,|\, p$, or $p = (x_i - a_i)q$ for some $q \in \mathbb{C}[x_i]$. So

$$\varphi(x_i - a_i)\varphi(q) = \varphi(p) = 0$$

Since K is a field, $\varphi_i(x_i - a_i) = 0$ or $\varphi_i(q) = 0$. By induction on $\deg p$, $\ker \varphi_i$ is a maximal ideal and hence a prime ideal (specifically, the ideal $(x_i - a_i)$).

It suffices now to show that $\ker \varphi_i \neq (0)$. For if so, M contains polynomials of the form $x_i - a_i$ for all $i \leq n$, and hence $M \subseteq (x_1 - a_1, \dots, x_n - a_n)$, as desired. Suppose $\ker \varphi_i = (0)$. Then

$$\mathbb{C}[x_i] \cong \varphi_i(\mathbb{C}[x_i]) =: \mathbb{C}[x] \subseteq K$$

So K contains a sub-$\mathbb{C}$-algebra isomorphic to the ring of complex polynomials in one variable. Since $\mathbb{C}[x]$ is an integral domain, denote its field of fractions

$$\mathbb{C}(x) = \left\{ \frac{p(x)}{q(x)} : p, q \in \mathbb{C}[x], q(x) \neq 0 \right\}$$

Since $\mathbb{C}(x)$ is a field, we can uniquely extend the homomorphism $\mathbb{C}[x] \hookrightarrow K$ to an injective homomorphism $\mathbb{C}(x) \hookrightarrow K$. Hence, K also contains a sub-$\mathbb{C}$-algebra isomorphic to $\mathbb{C}(x)$.

The field $\mathbb{C}[x_1, \dots, x_n]$, as a vector space over $\mathbb{C}$, has as a basis the set of all monic complex monomials in n variables. Since $\mathbb{C}[x_1, \dots, x_n] \twoheadrightarrow K$, K is also generated by a countable basis (in particular, the set of residues of monic complex n-polynomials). We will show that the $\mathbb{C}$-vector space $\mathbb{C}(x)$ contains an uncountable basis, and that this implies that $\mathbb{C}(x)$ is not isomorphic to any sub-$\mathbb{C}$-algebra of K.

Lemma 16.2. $\{\frac{1}{x-c}\}_{c \in \mathbb{C}}$ *form a linearly independent set in $\mathbb{C}(x)$.*

Proof. Suppose that

$$0 = f(x) = \sum_{j=1}^{n} \frac{\alpha_j}{x - c_j}$$

where the c_j are distinct and where some $\alpha_k \neq 0$ Then

$$\lim_{x \to c_k} |f(x)| = \left| \lim_{x \to c_k} \frac{\alpha_k}{x - c_k} + \lim_{x \to c_k} \sum_{j \neq k} \frac{\alpha_j}{x - c_j} \right| = \infty$$

and hence our set $\{\frac{1}{x-c}\}_{c \in \mathbb{C}}$ is indeed linearly independent. ■

Lemma 16.3. *Let V be a vector space which admits a finite basis $\{e_j\}$. Then every set $L \subseteq V$ of linearly independent vectors is up to countable.*

Proof. Let $V_n = \operatorname{span}(\{v_j\}_{j \leq n})$, and let $L_n = L \cap V_n$. Then $L_n \subseteq V_n$ is a linearly independent set of the finite vector space V_n, and hence is finite. But $L = \bigcup_{n \in \mathbb{N}} L_n$, and hence is countable or finite, as desired. ■

This completes our proof. ■

Lecture 17 — 11/2/10

Definition 17.1. We present some ideal-theoretic vocabulary. Let R be an integral domain, $a, b \in R$, $I, J \subseteq R$ ideals.

- a is a <u>unit</u> if $(a) = (1) = R$.
- b is a <u>multiple</u> of a, and a a <u>divisor</u> of b, if $(b) \subseteq (a)$.
- Similarly, J is a multiple of I and I is a divisor of J if $J \subseteq I$.
- b is a <u>proper divisor</u> of a if $(a) \subsetneq (b) \subsetneq (1)$.
- a is <u>associated</u> to b if $(a) = (b)$.

Definition 17.2. Let R be an integral domain. An element $p \in R$ is <u>prime</u> if $p \,|\, ab \implies p \,|\, a$ or $p \,|\, b$; that is, if (p) is a prime ideal.

Definition 17.3. Let R be an integral domain. An element $p \in R$ is irreducible if $p = a \cdot b \implies p \mid a$ or $p \mid b$. Equivalently, $p = a \cdot b$ implies that either a or b is associated to p, and the other element, either b or a, is a unit.

Note. If p is prime, then p is irreducible. Moreover, in a PID, if p is irreducible, then it is also prime.

Definition 17.4. Let $I, J \subseteq R$ be ideals in an integral domain. The greatest common divisor of I and J is a common divisor of I and J such that every other common divisor divides it. It is given by

$$\gcd(I, J) = (I, J)$$

the ideal generated by I and J.

Definition 17.5. Let R be an integral domain. A function

$$\sigma : R - \{0\} \longrightarrow \mathbb{N}$$

is called a size function on R.

Definition 17.6. A Euclidean domain is an integral domain R with a size function σ such that the Archimedean law holds.

Definition 17.7. The Archimedean law holds if $\forall a, b \in R$, $a, b \neq 0$, there is an equation in R of the form

$$a = mb + r$$

where either $r = 0$ or $\sigma(r) < \sigma(b)$.

Example.
1. $R = \mathbb{Z}$, $\sigma = |\,|$.
2. $R = K[t]$ for K a field, $\sigma = \deg$.
3. $\mathbb{Z}[i]$, $\sigma = \|\|$.

Example.

1. Consider the integral domain

$$\begin{aligned} R = \mathbb{Z}[\sqrt{-2}] &= \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\} \\ \subset F = \mathbb{Q}[\sqrt{-2}] &= \{a + b\sqrt{-2} : a, b \in \mathbb{Q}\} \end{aligned}$$

   R has a size function given by

$$\sigma(a + b\sqrt{-2}) = a^2 + 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2})$$

2. $R = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subset \mathbb{Q}\left[\frac{1+\sqrt{-3}}{2}\right]$

Example (Eisenstein Ring)**.** The Eisenstein Ring is the ring $R = \mathbb{Z}[e^{2\pi i/3}]$, the points of which correspond to the hexagonal lattice in $\mathbb{R}$. Its field of fractions $\mathbb{Q}[e^{2\pi i/3}]$ is dense in the complex plane.

The Eisenstein integers can be expressed as

$$a + b\omega := a + b\left(\frac{1}{2}(-1 + i\sqrt{3})\right)$$

and a size function on $\mathbb{Z}[e^{2\pi i/3}]$ is given by

$$\begin{aligned} \sigma(a + b\omega) &= |a + b\omega|^2 \\ &= (a + b\omega)(a + b\bar{\omega}) \\ &= a^2 + ab(\omega + \bar{\omega}) + b^2 \\ &= a^2 - ab + b^2 \end{aligned}$$

Proposition 17.8. *Every Euclidean domain is a PID.*

Proof. Let R be an ED, $I \subseteq R$ a nonzero ideal. Let $b \in I$ be such that $\sigma(b)$ is minimal among all nonzero elements of I. Suppose $a \in I$. Then by the Archimedean law, we have $b = ma + r$ for $\sigma(r) < \sigma(a)$ or $r = 0$. But we cannot have $\sigma(r) < \sigma(a)$ by minimality, so $r = 0$, and hence $I = (a)$, as desired. ■

Definition 17.9. A unique factorization domain R is an integral domain in which any nonzero element can be expressed as a product of irreducible elements uniquely, up to order and multiplication by units.

Note. We note that the factorization necessarily terminates. If a factorization never terminates, we are left with an ever-ascending chain of principal ideals each properly contained in the next

$$(a) \subsetneq (a_0) \subsetneq (a_1) \subsetneq \cdots$$

or

$$\cdots \mid a_2 \mid a_1 \mid a_0 \mid a$$

Hence, if this never occurs, factorization terminates.

Proposition 17.10. *Every PID is a UFD.*

Proof. Let R be a PID. First, we will show that there are no ever-ascending chains of ideals in R. Suppose otherwise. Then we have

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$$

and define

$$I_\infty = \bigcup_{i=0}^{\infty} I_i$$

We claim that I_∞ is an ideal. Say $x, y \in I_\infty$. Then $x \in I_m$ and $y \in I_n$ for some ideals I_m, I_n in our chain; assume WLOG that $m \leq n$. So $x, y \in I_n \subset I_\infty$, and hence $rx + sy \in I_n \subset I_\infty$.

Since R is a PID, we know that $I_\infty = (d)$ for some $d \in R$. But then $d \in I_n$ for some n. Then $(d) \subseteq I_n \subseteq I_\infty = (d)$. $\Rightarrow\Leftarrow$. Thus, $PIDs$ have terminating factorization.

It remains to be shown that such factorizations are unique. Let $a \in R, a \neq 0$, and suppose that

$$p_1 \cdots p_n = a = q_1 \cdots q_n$$

Write $p = p_1$. Since $p \mid a$, we have $p \mid q_1 \cdots q_n$. In a PID, every irreducible element is prime; hence, $p \mid q_i$ for some i. But since q_i is also prime, we have $p = q_i \cdot u$, where u is a unit. Proceeding by induction, this completes our proof. ■

Lecture 18 — 11/9/10

Remark. Recall that abelian groups are precisely the $\mathbb{Z}$-modules.

Definition 18.1. The exponent of an abelian group A is a positive integer e such that $\forall a \in A, e \cdot a = 0$. If we so desire, we can take e to be minimal.

Definition 18.2. A p-group is a finite group of order p^k for any $k \in \mathbb{N}$.

Theorem 18.3 (Fundamental Theorem of Finite Abelian Groups)**.** *Any finite abelian group A of order n has exponent n. We can factor*

$$n = p_1^{r_1} \cdots p_s^{r_s}$$

Then there are unique subgroups of A of exponent $p_i^{r_i}$ for $i = 1, \ldots, s$,

$$A_{p_i} \subset A$$

such that

$$A = \prod_{i=1}^{s} A_{p_i} = A_{p_1} \oplus \cdots \oplus A_{p_s}$$

where each A_{p_i} is a p_i-group. The A_{p_i} are called the p_i-primary components of A.

Remark.

1. We allow the possibility that some of the p-primary components of A are trivial, meaning that n was not minimal.
2. Since A is finite abelian, then the p-primary components are examples of p-Sylow subgroups (to be defined later).

Claim 18.4. *Let A be a finite abelian group of order n. Then A is a $\mathbb{Z}/n\mathbb{Z}$-module.*

Proof. Note that $n \cdot A = 0$. Let $a \in A$, and let

$$\mathbb{Z} \ni m \longmapsto \overline{m} \in \mathbb{Z}/n\mathbb{Z}$$

Define $\overline{m} \cdot a = m \cdot a$. Every representative of $\overline{m}$ is of the form $m' = m + tn$ for some $t \in \mathbb{Z}$, whereupon we have

$$m' \cdot a = (m + tn) \cdot a = m \cdot a + tn \cdot a = m \cdot a$$

and hence our module structure is well-defined, and, of course, necessarily unique. ■

Proof. (of Fundamental Theorem) Consider $\mathbb{Z}/n\mathbb{Z}$, where $n = pq$ for p, q prime, $p \neq q$. Let $\mathbb{Z}/n\mathbb{Z}$, $n = pq$ where $p, q \in \mathbb{P}, p \neq q$. We know that

$$\exists s, t \in \mathbb{Z} : 1 = sp + tq$$

Write

$$\epsilon_p = tq \qquad \epsilon_q = sp$$

In $\mathbb{Z}/n\mathbb{Z}$, we have

$$\epsilon_p \cdot \epsilon_q = 0$$

since $pq = n = 0$, and we say that ϵ_p, ϵ_q are orthogonal. Moreover, $1 = \epsilon_p + \epsilon_q \implies \epsilon_p = \epsilon_p^2 + \epsilon_p \epsilon_q$, and from symmetry and orthogonality, we get both

$$\epsilon_p^2 = \epsilon_p \qquad \text{and} \qquad \epsilon_q^2 = \epsilon_q$$

We say that ϵ_p and ϵ_q are idempotent. We refer to our formula

$$1 = \epsilon_p + \epsilon_q$$

as an orthogonal idempotent decomposition of unity.

Now let A be an abelian group of order n. Define

$$A_p := \epsilon_p \cdot A \qquad A_q := \epsilon_q \cdot A$$

We know from our decomposition that

$$a = \epsilon_p a + \epsilon_q a$$

so $A = A_p + A_q$. Suppose $a' \in A_p \cap A_q \subset A$. Then $a' = \epsilon_p a_p = \epsilon_q a_q$, for $a_p, a_q \in A$. We claim that $a' = 0$:

$$a' = \epsilon_p a_p = \epsilon_p^2 a_p = \epsilon_p \epsilon_q a_q = 0$$

So $A = A_p \oplus A_q$. We note that A_p is of exponent p:

$$pA_p = p \cdot \epsilon_p A = \{p \cdot tq \cdot a : a \in A\} = \{tn \cdot a : a \in A\} = 0$$

This same argument holds for $n = p^r q^s$, since p^r, q^s are coprime and hence $\exists u, v \in \mathbb{Z} : 1 = up^r + vq^s$. An inductive argument yields our desired result. ■

Definition 18.5. Let G be a finite group of order

$$|G| = p^e \cdot m$$

where p prime, $\gcd(m, p) = 1$. A p-Sylow subgroup of G is a subgroup $H \subseteq G$ of order $|H| = p^e$. Equivalently, it is a p-group of index coprime to p.

Theorem 18.6 (Sylow Theorems)**.** *Let G be a finite group of order $n = p^e \cdot m$, $\gcd(p, m) = 1$. Then*

1. *(Existence). The number ν_p of p-Sylow subgroups of G is such that*
   (a) $\nu_p \equiv 1 \pmod{p}$
   (b) $\nu_p \mid m$
2. *(Conjugacy). All p-Sylow subgroups of G are conjugate.*
3. *(Intersection). If $K \leq G$, there is a p-Sylow subgroup $H \leq G$ such that $K \cap H \subseteq K$ is a p-Sylow subgroup of K.*

Example. Consider D_{2p} for $p > 2$ prime. We can write

$$|D_{2p}| = p \cdot 2$$

where we have $e = 1, m = 2$. D_{2p} has at least one p-Sylow subgroup, namely the rotational subgroup $\langle r \rangle = C_p$. By the Sylow theorems, the total number ν_p of p-Sylow subgroups satisfies $\nu_p \mid 2$, and hence $\nu_p = 1$ or $\nu_p = 2$. Since also $\nu_p \equiv 1 \pmod{p}$, and since $p > 2$, we have must have $\nu_p = 1$.

We can also consider

$$|D_{2p}| = 2 \cdot p$$

and examine the 2-Sylow groups, which in this case are necessarily cyclic of order two. Our conditions on ν_2 are $\nu_2 \mid p$, which yields $\nu_2 = 1$ or $\nu_2 = p$, and $\nu_2 \equiv 1 \pmod{2}$, which yields no additional information. However, we know that each flip subgroup is a cyclic group of order 2, and hence $\nu_2 = p$.

Lecture 19 — 11/16/10

Definition 19.1. Let G be a group, $S \subseteq G$ a subset. The normalizer of S is the subgroup

$$N(S) = \{g \in G : gSg^{-1} = S\}$$

If $S \leq G$, then $N(S)$ is the largest subgroup of G such that $S \lhd N(S)$.

Proof. (of the Sylow Theorems). Define the collection

$$X = \{S \subseteq G : |S| = p^e\} \subseteq \mathcal{P}(G)$$

G acts on X by left-multiplication. Note that

$$\begin{aligned} |X| &= \binom{n}{p^e} \\ &= \frac{n \cdot (n-1) \cdots (n-k) \cdots (n-p^e+1)}{p^e \cdot (p^e-1) \cdots (p^e-k) \cdot \cdots \cdot 1} \\ &= \prod_{k=0}^{p^e-1} \frac{n-k}{p^e-k} \end{aligned}$$

We claim that if $p \mid n-k$, then also $p \mid p^e - k$ the same number of times. Let us write $k = p^f l$, where $p \nmid l$. Then $f < e$. Hence, $p^f \mid n-k$ and $p^f \mid p^e - k$, but $p^{f+1} \nmid n-k$ and $p^{f+1} \nmid p^e - k$. Thus, $|X|$ is coprime with p. We can decompose X into disjoint orbits

$$X = \mathcal{O}_1 \sqcup \cdots \sqcup \mathcal{O}_\mu$$

And we know that

$$|X| = \sum |\mathcal{O}_i| \not\equiv 0 \pmod{p}$$

So there is one orbit $\mathcal{O}$ with order not divisible by p. By definition, G acts on $\mathcal{O}$ transitively. Take $U \in \mathcal{O}$, (so $U \subseteq G$). Consider the stabilizer

$$G_U = \{g \in G : g \cdot U = U \subseteq G\} \leq G$$

The elements of G_U fix U, but may "rearrange" the elements of U.

Consider, then, the action of $G_U \circlearrowleft U \subseteq G$ by left-multiplication. The orbits under this action are the right-G_U-cosets. Note that the stabilizer for any $u \in U$ is trivial, which means there is only one orbit, and hence $|U| = |G_U|$. Alternatively, we have, for some $M \in \mathbb{N}$,

$$p^e = |U| = \sum |G_U u| = M|G_U|$$

By the orbit-stabilizer theorem, we have

$$|G| = |G_U| \cdot |\mathcal{O}|$$

where $|G_U|$ is a power of p, $|\mathcal{O}|$ is not divisible by p, and $|G| = p^e \cdot m$ such that $m \not\equiv 0 \pmod{p}$. So $|G_U| = p^e$ is our p-Sylow subgroup, and $|\mathcal{O}| = m$.

The subgroups conjugate to $H := G_U$ are p-Sylow and correspond bijectively to the points of $\mathcal{O}$. For say $U, U' \in \mathcal{O}$. Then $\exists g \in G : gU = U'$. We claim that g conjugates G_U and $G_{U'} =: H'$; we have

$$gHg^{-1}U' = gHg^{-1}gU = gHU = gU = U'$$

Conversely, if $H' = gHg^{-1}$, take $U' = gU$. Then we have $H' = G_{U'}$.

Let $K \leq G$ be any subgroup. Restrict the action of G on $\mathcal{O}$ to an action K on $\mathcal{O}$. (Note that we have chosen one orbit $\mathcal{O}$ out of potentially many possibilities; we will show later that there is only one such viable orbit.) We can show there exists one orbit $\mathcal{O}_K$, $|\mathcal{O}_K| \not\equiv 0 \pmod{p}$ (since $|\mathcal{O}|$ is coprime with p and $\mathcal{O}$ is a disjoint union of K-orbits).

We repeat our argument for K. Write

$$|K| = p^{e'} \cdot m'$$

where $\gcd(m', p) = 1$. Note that $\mathcal{O}_K \subseteq \mathcal{O}$. So, choosing $U_K \in \mathcal{O}_K$, and recalling the action of $K \leq G$ on it, we have

$$|K| = |K_{U_K}| \cdot |\mathcal{O}_K|$$

As before, $H_K := K_{U_K}$ is a p-Sylow subgroup of K. We can also consider $U_K \in \mathcal{O}$, where it is acted on by G. Then we find that

$$K_{U_K} = G_{U_K} \cap K$$

which proves *(3)*.

Since $U_K \in \mathcal{O}$, the stabilizer G_{U_K} is conjugate to the p-Sylow $H \leq G$ described earlier. Thus, given any $K \leq G$ and recalling our p-Sylow $H \leq G$, then there exists a p-Sylow conjugate to H such that its intersection with K is p-Sylow in K.

Now apply this result to K a p-Sylow in G. There is a p-Sylow H' in G conjugate to H such that $H' \cap K$ is a p-Sylow of K. So $H' = K$. Hence all p-Sylow groups are conjugate, and hence our choice of orbit $\mathcal{O}$ is unique; this proves *(2)*.

Now define

$$Y = \{H \leq G : |H| = p^e\}$$

G acts on Y by conjugation. Let $H \in Y$. The normalizer of H is given by

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

and since all p-Sylows are conjugate, we have that $G/N(H) \cong Y$ by the map

$$gG_H \longmapsto gHg^{-1} = gN(H)$$

Thus we have

$$\nu_p = |Y| = [G : N(H)]$$

and hence $\nu_p \,|\, m$, since $H \lhd N(H)$ and $|H| = p^e$. Restrict the action of G to H. Let $H' \in Y$ such that H fixes H'. Then both

$$H \leq N(H') \qquad \text{and} \qquad H' \lhd N(H')$$

H and H' are p-Sylow groups in $N(H')$ and hence conjugate; since H' is normal, $H = H'$. So $\{H\}$ is the only singleton orbit of the action under H. Since all other orbits have order dividing $|H| = p^e$,

$$\nu_p = |Y| \equiv 1 \pmod{p}$$

This completes the proof. ∎

Example. Let G be a group, $|G| = 15 = 5 \cdot 3$. The 3-Sylows and 5-Sylows are all cyclic. Let us first determine the 3-Sylows subgroups. We know that $\nu_3 \equiv 1 \pmod 3$ and $\nu_3 \mid 3$; hence, $\nu_3 = 1$. Since there is only one, it is normal. We have the same result for the 5-Sylows. So $G \cong C_3 \times C_5$.

Example. Now take $|G| = 6$. We have $\nu_3 = 1$, yielding $C_3 \lhd G$. If $\nu_2 = 1$, we get $C_6 \lhd G$, and if $\nu_2 = 3$, we get $S_3 \leq G$.

Lecture 21 — 11/23/10

Definition 21.1. Let M be a module. We call a subgroup $N \leq M$ a submodule if it is closed under scalar multiplication. Note that a submodule is also a module.

Definition 21.2. Let M be a module, $M' \leq M$ a submodule. The quotient group M/M' is equipped with scalar multiplication, defined in the natural way by

$$r(m + M') = rm + M'$$

for $r \in R$. The resulting module M/M' is called a quotient module.

Claim 21.3. *The natural map $M \xrightarrow{\pi} M/M'$ is an R-homomorphism.*

Proof. This results directly from the definitions. $\forall r \in R$, $\forall m \in M$,

$$\pi(rm) = rm + M' = r(m + M') = r\pi(m)$$ ∎

Definition 21.4. Consider the sequence of homomorphisms and R-modules

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

This sequence is called exact if $\ker(g) = \operatorname{im}(f)$. More generally, a sequence

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} M_n$$

is exact at M_i if $\ker(f_{i+1}) = \operatorname{im}(f_i)$. This sequence is exact if it is exact at every M_i.

Example. Consider an R-module homomorphism

$$M_1 \xrightarrow{h} M_2$$

The image $h(M_1)$ is indeed an R-module since $\forall r \in R$, $rh(M_1) = h(rM_1)$. Taking the quotient of M_2 with $h(M_1)$ yields the exact sequence

$$M_1 \xrightarrow{h} M_2 \xrightarrow{\pi} M_2/h(M_1)$$

Observation 21.5. Consider a sequence

$$0 \longrightarrow M_1 \xrightarrow{f} M_2$$

This sequence is exact iff f is injective. Similarly, a sequence

$$M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

is exact iff g is surjective.

Definition 21.6. A short exact sequence is an exact sequence of the form

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

If we consider $M_1 \subseteq M_2$, we get $M_3 \cong M_2/M_1$ (or, more generally, $M_3 \cong M_2/f(M_1)$).

Observation 21.7. If the sequence

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

is exact, we know that $M_3 \cong M_2/f(M_1)$. On the other hand, if the sequence

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

is exact, then $M_1 \cong \ker(g)$.

Remark. Recall that a free R-module of rank n is an R-module

$$F \cong R^n = \underbrace{R \oplus \cdots \oplus R}_{n}$$

which has a linearly independent finite generating set (or basis) $\{\epsilon_i\}_{i=1}^n$, where we can take

$$\epsilon_i = (\underbrace{0, 0, \ldots, 1}_{i}, \ldots, 0)$$

This is the unique R-module such that for any module M and elements $\{m_i\}_{i=1}^n \in M$, there exists a unique R-homomorphism $g : F \to M$ given by $\epsilon_i \mapsto m_i$.

Observation 21.8. Suppose that the $\{m_i\}_{i=1}^n$ above form a generating set for M, which is to say that $\forall m \in M$, $\exists r_i \in R$ such that

$$m = \sum_{i=1}^{n} r_i m_i$$

not necessarily uniquely. Equivalently, our map above $g : F \to M$ given by $\epsilon_i \mapsto m_i$ is surjective, which is to say that the sequence

$$F \xrightarrow{g} M \longrightarrow 0$$

is exact.

Definition 21.9. The kernel of the map above is called the R-module of relations. We note that

$$\ker(g) = \left\{(r_1, \ldots, r_n) \in F : \sum r_i m_i = 0\right\}$$

is in correspondence with the linear combinations of $\{m_i\}$ that are 0.

Example. Let $R = \mathbb{Z}$, $F = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$. The element $m := 1 \in M$ generates M. m is not a free generator; for instance, $nm = 0$ is a relation on M. The quotient map $F \to M$ yields the exact sequence

$$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

and we find that $\ker(\pi) = n\mathbb{Z}$.

Observation 21.10. We have the exact sequence

$$\ker(g) \leq F \xrightarrow{g} M \longrightarrow 0$$

Suppose that $\ker(g)$ has a finite generating set $\{\mu_j\}_{j=1}^q$. Let F' be the free R-module of rank q with basis ϵ_j', and let $A : F' \to \ker(g)$ be the unique map given by $\epsilon_j' \mapsto \mu_j$. Then $\operatorname{im}(A) = \ker(g)$, which yields an exact sequence

$$F' \xrightarrow{A} F \xrightarrow{g} M \longrightarrow 0$$

We call F' the free R-module of relations and F the free R-module of generators. As before, the map A completely describes M.

Definition 21.11. A presentation of an R-module M is an R-homomorphism $A : F' \to F$ such that $F/A(F') \cong M$, or equivalently, such that there exists an R-homomorphism $g : F \to M$ making

$$F' \xrightarrow{A} F \xrightarrow{g} M \longrightarrow 0$$

exact. To encompass our previous discussion, a presentation is a system of generators $\{m_i\}_{i=1}^n \in M$ and a system of relations $\{\sum_{i=1}^n r_{i,j} m_i\}_{j=1}^q \in M$, such that the maps $\epsilon_j' \mapsto \sum_{i=1}^n r_{i,j}\epsilon_i$ and $\epsilon_i \mapsto m_i$ given by A and g respectively yield an exact sequence

$$F' \xrightarrow{A} F \xrightarrow{g} M \longrightarrow 0$$

Since $F' = R^q$ and $F = R^n$, we have

$$(r_{i,j}) = A \in \operatorname{Hom}_R(R^q, R^n) \cong M_{n\times q}(R)$$

Note. Given a matrix $A \in M_{n\times q}(R)$, we get an R-module M with generating set of n elements and system of relations generated by q elements. However, different matrices A may give the same module M.

Definition 21.12. A cyclic R-module is an R-module with a single generator.

Example. Let M be a cyclic R-module with generator $m \in M$. Let $g : R \to M$ be the map given by $r \mapsto rm$, which is certainly surjective, and hence yields exactness of the sequence

$$R \xrightarrow{g} M \longrightarrow 0$$

$\ker(g)$ is an ideal in R. If it is principal, then $n = 1$ and $q = 1$, so A is a 1×1 matrix. So $A = (\alpha), \alpha \in R$, and we have that

$$R \xrightarrow{\cdot\alpha} R \xrightarrow{g} M \to 0$$

is exact, which yields $M \cong R/\alpha R$.

However, $\ker(g)$ is not necessarily principal. Consider, for instance, $R = F = \mathbb{C}[X, Y]$, $M = \mathbb{C}$, where scalar multiplication is given by $zm = zm$, $Xm = 0$, $Ym = 0$. Define $g : R \to M$ by $p(X, Y) \mapsto p_0 m$, which is certainly surjective. Then

$$F \xrightarrow{g} M \longrightarrow 0$$

is exact, with $\ker(g) = (X, Y)$. Then we have $F' = R^2$, along with an exact sequence

$$F' \xrightarrow{A} F \xrightarrow{g} M \longrightarrow 0$$

where A is given by $\epsilon_1' \mapsto X$, $\epsilon_2' \mapsto Y$, and hence has the form

$$A = (X, Y)$$

Lecture 22 — 11/30/10

Recall that a finitely-generated R-module M has a presentation if there exists an exact sequence

$$F' \xrightarrow{f} F \xrightarrow{g} M \longrightarrow 0$$

where $F' = R^n$, $F = R^m$, with bases $\{\epsilon_i'\}$ and $\{\epsilon_j\}$ respectively, and where g maps $\{\epsilon_j\}$ to a generating set of M. Then f is given by some $m \times n$ matrix in R, which is referred to as the presentation of M. Note that a change of basis for F' and for F changes the presentation matrix, but not the presented module M.

Example. Let $R = \mathbb{Z}$, and consider the presentation

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

We have $F' = F = \mathbb{Z}^2$, with bases $\{\epsilon_1', \epsilon_2'\}$ and $\{\epsilon_1, \epsilon_2\}$ respectively, and our matrix provides

$$\begin{aligned} \epsilon_1' &\longmapsto 2\epsilon_1 \\ \epsilon_2' &\longmapsto \epsilon_1 + 2\epsilon_2 \end{aligned}$$

So our module is given by

$$\begin{aligned} \epsilon_1\mathbb{Z} \times \epsilon_2\mathbb{Z} &= \mathbb{Z}^2/(\epsilon_1'\mathbb{Z}, \epsilon_2'\mathbb{Z}) \\ &= \mathbb{Z}^2/(2\epsilon_1\mathbb{Z}, (\epsilon_1 + 2\epsilon_2)\mathbb{Z}) \end{aligned}$$

Observation 22.1. Suppose the exact sequence of the presentation of M is given by

$$R^n \xrightarrow{A} R^n \longrightarrow M \longrightarrow 0$$

and we have

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

Then we find that

$$M = R/d_1R \times R/d_2R \times \cdots \times R/d_nR$$

Note that we can have this result even when the two free modules are not of equal rank. If we can show that, for some ring R, every matrix is diagonalizable, then we realize every finitely-presented R-module as a product of cyclic R-modules.

Note. Recall the elementary row and column on matrices:

1. Add a scalar multiple of one row to another, or of one column to another.
2. Interchange two rows or two columns.
3. Multiply a row or a column by a unit.

These operations do not change the image of a matrix, and hence when applied to a presentation, do not change the presented module.

Theorem 22.2. *Any $m \times n$ matrix A with entries in $\mathbb{Z}$ is diagonalizable as*

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

Where the d_i are nonnegative and $d_i \mid d_{i+1}$.

Proof. This proof proceeds by induction. First, by interchanging rows and columns and negating as necessary, we take $|a_{1,1}|$ to be minimal among all values $a_{i,j}$.

Choose a nonzero entry $a_{i,1}$ in the first column, with $i > 1$ (if such an entry does not exist, move on). By the division theorem,

$$a_{i,1} = a_{1,1}q + r$$

where $0 \leq r < a_{i,1}$. Subtract q times the 1st row from the ith row, which changes $a_{i,1}$ to r. If $r = 0$, then we have produced a zero in the ith row of the first column. If $r \neq 0$, then $r < a_{i,1}$, so we return to the first step and move r (or some entry that has been produced that is smaller than r) to $a_{1,1}$. Eventually, we must produce a column of all 0's, because $a_{1,1}$ is reduced each time, and cannot be reduced past $a_{1,1} = 1$. By an analogous method, we reduce the first row to all 0's.

We are now left with the matrix

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

To achieve our desired divisibility, we want to have $d_1 \mid a'$ for every entry a' in A'. Suppose $\exists a_{i,j},\ i,j \neq 1$ such that $d_1 \nmid a_{i,j}$. Add the jth column of A to the 1st column; this produces $a_{i,j}$ in the first column. Applying the division theorem produces a smaller entry; returning to our first step and repeating, we eventually (after finitely many steps) get a remainder of zero, which yields our desired divisibility. Finally, induction on m, n completes the proof. ■

Observation 22.3. The statement of the theorem above also holds for any Euclidean domain, which, like the ring of integers, satisfies the Archimedean law.

Theorem 22.4 (Fundamental Theorem of Finitely-Generated Abelian Groups)**.** *Any finitely-generated abelian group is isomorphic to* $\mathbb{Z}^k \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ *where* $d_i \mid d_{i+1}$ *and each* $d_i \neq 0$.

Proof. Note that we assume that every finitely-generated $\mathbb{Z}$-module has a finite presentation (this stems from the fact that $\mathbb{Z}$ is a noetherian ring). Every finitely-generated abelian group is a finitely-generated $\mathbb{Z}$-module. Hence, by our assumption, it has a finite presentation, which by diagonizability, can be expressed in the "better diagonal" form shown above.

We can drop any column of all 0's from this matrix, along with any row or column with diagonal entry 1 (the former represents a trivial relation; the latter, a trivial generator). This yields a matrix given by a diagonal submatrix followed by rows of 0's. The module presented by the diagonal portion is $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$; the module presented by the rows of 0's is $\mathbb{Z}^k$. ■

Lemma 22.5 (Splitting Lemma)**.** *Let*

$$0 \longrightarrow A \xrightarrow{q} B \xrightarrow{r} C \longrightarrow 0$$

be a short exact sequence. TFAE:

1. *Left split:* $\exists t : B \to A$ *such that* tq *is the identity on* A.
2. *Right split:* $\exists u : C \to B$ *such that* ru *is the identity on* C.
3. *Direct sum:* $B \cong A \times C$*, where* q *is the natural injection into* A *and* r *is the natural projection onto* C.

Definition 22.6. Let

$$0 \longrightarrow A \xrightarrow{q} B \xrightarrow{r} C \longrightarrow 0$$

be a short exact sequence. If any of the above conditions hold, we say the sequence is split.

Lecture 23 — 12/2/10

Observation 23.1. We know that a finite abelian group A is the direct sum of its p-primary components; that is,

$$A \cong \prod_{p \in \mathbb{P}} A_p = A_2 \times A_3 \times A_5 \times \cdots$$

But A is also a $\mathbb{Z}$-module, and hence

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots$$

where $|A| = \prod_i d_i$ and $d_i \mid d_{i+1}$. Combining these two decompositions, we get

$$\begin{aligned} A_2 &\cong \mathbb{Z}/2^{e_{2,1}}\mathbb{Z} \times \mathbb{Z}/2^{e_{2,2}}\mathbb{Z} \times \cdots \\ A_3 &\cong \mathbb{Z}/2^{e_{3,1}}\mathbb{Z} \times \mathbb{Z}/2^{e_{3,2}}\mathbb{Z} \times \cdots \\ &\vdots \end{aligned}$$

Observation 23.2. Now take $R = k[T]$ for k a field; this is the polynomial ring in one variable T. $k[T]$ is a Euclidean domain, given by size function

$$\deg : k[T] - \{0\} \longrightarrow \mathbb{N}$$

and we can write

$$p(T) = m(T)q(T) + r(T)$$

and $\deg r < \deg q$ if $r \neq 0$. Hence, matrices with coefficients in $k[T]$ can be divisibly diagonalized.

Let M be any finitely-presented $k[T]$-module. Then

$$M = k[T]/(f_1) \times k[T]/(f_2) \times \cdots \times k[T]^r$$

where the f_i's are monic and $f_i \mid f_{i+1}$. Now consider some specific quotient

$$k[T]/(f) = k[T]/f \cdot k[T]$$

We can uniquely factor f as

$$f = g_1^{e_1} \cdot g_2^{e_2} \cdots g_\nu^{e_\nu}$$

where the g_i's are distinct monic irreducible polynomials, $e_i \geq 1$. By linear independence,

$$(1) = (g_i^{e_i}, g_{i+1}^{e_{i+1}} \cdots g_\nu^{e_\nu})$$

and by the Chinese Remainder Theorem,

$$\begin{aligned} k[T]/(f) &= k[T]/(g_1^{e_1} \cdots g_\nu^{e_\nu}) \\ &= k[T]/(g_1^{e_1}) \cdots k[T]/(g_\nu^{e_\nu}) \end{aligned}$$

Observation 23.3. Now let V be a $k[T]$-module; it is also a vector space over k. Suppose $\dim V$ is finite. So we can write

$$V \cong k[T]/(h_1^{e_1}) \times \cdots \times k[T]/(h_\mu^{e_\mu})$$

If instead we take V to be any finite-dimensional vector space over k and $T : V \to V$ any k-linear endomorphism. Then V has a $k[T]$-module structure

$$p(T)(v) = \left(\sum_{i=1}^{d} a_i T^i\right)(v) = \sum_{i=1}^{d} a_i T^i(v)$$

So we can express T as a block matrix

$$T = \begin{pmatrix} \boxed{B_1} & & & \\ & \boxed{B_2} & & \\ & & \ddots & \\ & & & \boxed{B_\mu} \end{pmatrix}$$

Let us decompose T. Take $V = k[T]/(f)$, where

$$f(T) = T^n + a_{n-1}T^{n-1} + a_{n-2}T^{n-2} + \cdots + a_0$$

for $a_i \in k$. V has a basis of $1, T, T^2, \ldots, T^{n-1}$, and so we can express our endomorphism T as

$$T = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ 0 & 0 & 1 & \ldots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

This is known as rational canonical form.

Theorem 23.4. *Every endomorphism $T : V \to V$ of a finite-dimensional vector space can be expressed as a matrix in rational canonical form.*

Observation 23.5. Now take $k = \mathbb{C}$, $k[T] = \mathbb{C}[T]$. The irreducible polynomials have the form $T - \lambda$, so we take

$$V = \mathbb{C}[T]/(T - \lambda)^e$$

Writing $X = T - \lambda$, we have

$$\mathbb{C}[X]/(X^e) = \mathbb{C}[T]/(T - \lambda)^e$$

V has a basis $1, X, X^2, \ldots, X^{e-1}$. Hence, we can write

$$X = \begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix}$$

Since $T = X + \lambda I$, we get

$$T = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix}$$

This is called a Jordan block. Recalling our decomposition of any vector space, we get the upcoming theorem.

Theorem 23.6. *If $T : V \to V$ is a linear endomorphism of finite-dimensional vector spaces over an algebraically closed field, there exists a basis such that T can be expressed in* Jordan normal form.

Theorem 23.7. *A finite abelian group A is cyclic iff*

$(*)$ *$\forall p \in \mathbb{P}$, $\{a \in A : pa = 0\}$ is either trivial or cyclic of p-power order.*

Proof. We can decompose A into p-primary subgroups

$$A \cong A_{p_1} \times A_{p_2} \times \cdots \times A_{p_\nu}$$

where $A_{p_i} \neq \{0\}$. We can further decompose

$$A_p = \mathbb{Z}/p^{\alpha_1} \times \cdots \times \mathbb{Z}/p^{\alpha_n}$$

and it is clear, then, that

$$\begin{aligned} \{a \in A : pa = 0\} &= \{a \in A_p : pa = 0\} \\ &= \prod_{i=1}^{n} \{a_i \in \mathbb{Z}/p^{\alpha_i} : pa_i = 0\} \end{aligned}$$

which yields our condition $(*)$. On the other hand, if A satisfies $(*)$,

$$A_{p_i} = \mathbb{Z}/p^{\alpha_i}$$

for $\alpha_i \geq 0$. Moreover, we know

$$\mathbb{Z}/p_1^{\alpha_1} \times \mathbb{Z}/p_n^{\alpha_n} \cong \mathbb{Z}/p_1 p_2 \cdots p_n$$

which exhibits cyclicity, as desired. ∎

Corollary 23.8. *Any finite subgroup of the multiplicative group of a field is cyclic.*

Proof. Let F be a field. We know $F^* \leq F$ is abelian. Choose some finite subgroup $A \leq F^*$. We will show that it satisfies $(*)$. Every element of the set

$$\{a \in A : a^p = 1\}$$

is a root of the polynomial $X^p - 1$, of which there are maximally p. This group is a p-group but has order $\leq p$; hence, it is either trivial or of order p and hence cyclic. Our result follows from the previous theorem. ∎

Corollary 23.9. *Let $\mathbb{F}_q$ for q prime. Then $\mathbb{F}_q^*$ is cyclic of order $q - 1$.*