MATH H333 (Algebra I) Lecture Notes

Guilherme Zeus Dantas e Moura
gdantasemo@haverford.edu

Haverford College
Fall 2020
Last updated: December 29, 2020

This is Haverford College's undergraduate MATH H333, instructed by Tarik Aougab. All errors are my responsability.

Use these notes only as a guide. There is a non-trivial chance that some things here are wrong or incomplete (especially proofs).

This class is being taught remotely via Zoom.

Contents

1 Binary Operations (September 09, 2020)

1.1 Why Algebra?

Algebra is the study of symmetry. An object has a symmetry when we can do something to it (transform it in some way) and without changing its appearance.

Example 1.1

A circle has a rotational symmetry: if we rotate the circle about its center, we get the same circle.

Example 1.2

The algebraic equation $x^2 + y^2 + z^2 - 3xyz = 0$ has a symmetry: for example, we can change the roles of x and z, which gives us the same equation.

Symmetry appears all over Mathematics, so Algebra is a prevalent topic abroad Mathematics.

1.2 Places where Algebra arises in Mathematics

Number Theory. The following theorem will be proven in this course.

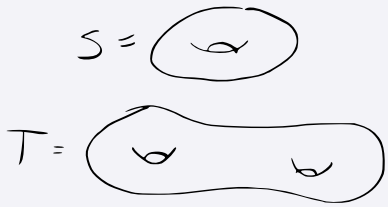
Theorem 1.1 (Fermat's Little Theorem)

Let p be a prime integer number. Let a be a positive integer number. Then, $a^p - a$ is a multiple of p.

Topology.

Theorem 1.2

There is no continous bijection $f : S \to T$.



Sketch. Associate a "group" to S and another to T. A continous bujection would send the S-group perfectly to the T-group. But the two groups are different.

1.3 Binary Operations

Definition 1.3

If S is a set, then a *binary operation* on S is a function $f : S \times S \to S$. Here, $S \times S = \{(a, b) \mid a, b \in S\}$.

Example 1.3

If $S = \mathbb{R}$, then $f(a, b) = a + b$ and $g(a, b) = a \cdot b$ are binary operations.

Example 1.4

If $S = \mathbb{N}$, then $h(a, b) = a - b$ is not a binary operation.

Definition 1.4

A binary operation $f : S \times S \to S$ is *associative* if, for all $a, b, c \in S$,

$$f(f(a, b), c) = f(a, f(b, c)).$$

Example 1.5

If $S = \mathcal{M}_n(\mathbb{R})$, then $f(A, B) = AB$ is an associative binary operation.

Example 1.6

If $S = \mathbb{R}$, then $f(a, b) = a - b$ is a non-associative binary operation.

A key concept in Algebra is *transformation*.

Example 1.7

Let S be a non-empty section. Define $g(S) = \{T : S \to S\}$. Then, composition is an associative binary operation on $g(S)$, i.e., $f(T_1, T_2) = T_1 \circ T_2$ is an associative binary operation on $g(S)$.

2 Groups (September 11, 2020)

In the last class, we focused on binary (associative) operations.

2.1 Defining Groups

Definition 2.1 (Notation)

If $a, b \in S$, then ab or $a \cdot b$ will commonly be used to denote $f(a, b)$. We will also commonly call this operation a *product*.

Associativity allows us to be less careful when writing down long products.

Example 2.1

In general, $a_1a_2a_3a_4a_5a_6a_7$ has no meaning. However, if the binary opperation is associative, no matter in which order we do the product, there will be no ambiguity about what value the expression have.

Definition 2.2

A binary operation on S is called *commutative* if for all $a, b \in S$, $ab = ba$ holds.

Example 2.2 (*i*) $(\mathbb{R}, +)$, $(\mathbb{C}, \cdot)$ have commutative binary operations.
(*ii*) $(\mathcal{M}_n(\mathbb{R}),$ matrix multiplication) has a non-commutative operation.
(*iii*) $(\mathbb{R},$ distance), i.e, $f(a, b) = |a - b|$, has a commuative, but non-associative operation.

Definition 2.3

Given S equipped with a binary opperation, we say $(S, \cdot)$, has an identity element if there exists $e \in S$ such that, for all $a \in S$, $a \cdot e = e \cdot a = a$ holds.

Example 2.3

(*i*) $(\mathbb{R}, +)$ has 0 as an identity.
(*ii*) $(\mathbb{R}, \cdot)$ has 1 as an identity.
(*iii*) $(\mathcal{M}_n(\mathbb{R}),$ matrix multiplication) has I_n as an identity.

Definition 2.4

An element a of $(S, \cdot)$, that has an identity element (which we are going to call e), is called invertible if there exists $b \in S$ so that $ab = ba = e$.

Example 2.4

(*i*) Every element of $(\mathbb{R}, +)$ is invertible.
(*ii*) Every element, except 0, of $(\mathbb{R}, \cdot)$ is invertible.
(*iii*) Some elements, but not all, of $\mathcal{M}_n(\mathbb{R})$, equipped with matrix multiplication, are invertible.

Definition 2.5

A *group* is a set $(G, \cdot)$ with a binary opperation so that:

(*i*) The binary opperation is associative.
(*ii*) There exists an identity element in G.
(*iii*) Every element in G is invertible.

If $\cdot$ is commutative, G is called an *abelian group*.

Example 2.5

(*i*) $(\mathbb{R}, +)$ is a group.
(*ii*) $(\mathbb{C}, +)$ is a group.
(*iii*) $(\mathbb{Z}, +)$ is a group.
(*iv*) $(\mathbb{R}\backslash\{0\}, \cdot)$ is a group.
(*v*) $(\mathbb{C}\backslash\{0\}, \cdot)$ is a group.
(*vi*) $(\mathbb{Z}\backslash\{0\}, \cdot)$ is not a group, because 2 does not have an inverse element.
– However, $(\mathbb{Q}\backslash\{0\}, \cdot)$ is a group.
(*vii*) $\mathcal{M}_n(\mathbb{R})$, equipped with matrix multiplication is not a group, because the zero matrix does not have an inverse element.
– However, if we define $GL_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \ : \ A \text{ is invertible}\}$, then $GL_n(\mathbb{R})$, equipped with matrix multiplication is a group.[a]
(*viii*) Define $D_8 = \{\text{affine bijections } T : \mathbb{R}^2 \to \mathbb{R}^2 \text{ such that } T(\mathcal{S}) = \mathcal{S}\}$, where $\mathcal{S} = \{(0,0), (0,1), (1,0), (1,1)\}$, also known as the standard unit square.

[a] It is important to prove that matrix multiplication is closed under $GL_n(\mathbb{R})$. In addition, this is the first example of a non-abelian group.

3 Subgroups (September 14, 2020)

Let's look more closely to $D_8 = \{\text{affine bijections } T : \mathbb{R} \to \mathbb{R} \text{ such that } T(\mathcal{S}) = \mathcal{S}\}$.

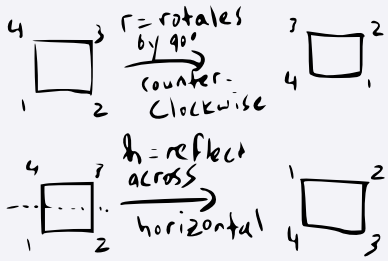
Proposition 3.1

D_8 is a group. The order of the group D_8 is 8.

Proposition 3.2

Let $r, h \in D_8$ be described as follows:

(*i*) r denotes the rotation of $\mathcal{S}$ by 90°, counter-clockwise.
(*ii*) h denotes the reflect across the horizontal perpendicular bisector.



If $\phi \in D_8$, then ϕ can be expressed as $\phi = \phi_n \circ \phi_{n-1} \circ \cdots \phi_1$, where $\phi_i = h$ or $\phi_i = r$, for all i.

The proposition above should resemble the concept of basis in Linear Algebra. In some sense, h and r gererate the group D_8.

Example 3.1

Let d be the reflection through the diagonal line through $(0,0)$ and $(1,1)$. We have $d = h \circ r \circ r \circ r = hr^3$.

Example 3.2

Let v be the reflection though the vertical perpendicular bisector. We have $v = hr^2$.

Note that $h^2 = r^4 = e$, and $2 \cdot 4 = 8$, which is the number of elements in D_8. What a coincidence, isn't it?

Definition 3.3

A *subgroup* H of a group $(G, \cdot)$ is a subset of G that is a group itself, with respect to the same operation $\cdot$.

Example 3.3

(*i*) If G is a group, it has an identity, say e. Then $\{e\}$ is a subgroup of G.
(*ii*) G is always a subgroup of G.

Lemma 3.4

Given a a group G, a non-empty subset $H \subset G$ is a subgroup of G if, and only if, both following conditions are met:

(*i*) $ab \in H$, for all $a, b \in H$.
(*ii*) $a^{-1} \in H$, for all $a \in H$.

Example 3.4

$2\mathbb{Z} = \{\text{even integers}\}$ is a subgroup of $(\mathbb{Z}, +)$.

Definition 3.5 (Symmetric group on n elements)

Given $n \in N$, define $S_n = \{\text{bijections } \tau : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}\}$, equipped with composition.

Example 3.5

Let $n = 5$, then consider $\tau : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$. Then $\tau \in S_5$.

Alternatively, we can use the following notation for $\tau = (13)(24)(5)$, which is called *cycle notation*.

Example 3.6

Consider $\tau' : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$. We can write $\tau' = (124)(35)$, using cycle notation.

Example 3.7

Consider $\tau'' : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$. We can write $\tau'' = (12345)$, using cycle notation.

Remark. Cycle notation is "not unique", e.g., $(12345) = (34512)$.

4 Integers (September 16, 2020)

Proposition 4.1

S_n us a finite group, and $|S_n| = n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$.

Proof. An arbitrary element $\tau \in S_n$ is described by determining $\tau(1), \tau(2), \ldots, \tau(n)$. We have n choices for $\tau(1)$; after that, we have $n-1$ choices for $\tau(2)$; ...; after that, we have 1 choice for $\tau(n)$. □

Example 4.1

Suppose $q, p \in S_5$, $q = (14325)$ and $p = (15)(34)$. Determine qp in cycle notation.

Answer (Cheat). $qp = (14325)(15)(34)$.

Answer (More useful). $qp = (425)$.

Definition 4.2

Given $\tau \in S_n$, define M_τ as a $n \times n$ matrix obtained by permuting the rows of I_n in accordance with τ.

Example 4.2

If $\tau \in S_4$, $\tau = (134)$, then

$$M_\tau = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Given $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$, we have $M_\tau \vec{v} = \begin{pmatrix} x_4 \\ x_2 \\ x_1 \\ x_3 \end{pmatrix}$.

Theorem 4.3

Given $\tau \in S_n, \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, then $M_\tau \vec{x} = \begin{pmatrix} x_{\tau^{-1}(1)} \\ x_{\tau^{-1}(2)} \\ \vdots \\ x_{\tau^{-1}(n)} \end{pmatrix}$.

Theorem 4.4

$\det(M_\tau) = \pm 1$.

Theorem 4.5

Given $p, q \in S_n$, then $M_{pq} = M_p M_q$.

Definition 4.6

The *sign of* $\tau \in S_n$ is either ± 1, and it is just $\det(M_\tau)$.

Problem 4.1

If $G = (\mathbb{Z}, +)$, what are all subgroups of G?

Solution. Let H be a subgroup of G. $0 \in H$, because 0 is the identity element.

If $H = \{0\}$, we have a group – note that $H = 0\mathbb{Z}$. Otherwise, H has an element distinct from 0. Since $a \in H \iff -a \in H$, then there is a positive integer in H.

Let h be the smallest positive integer in H. Since addition is a binary opperation in H, we have $h\mathbb{Z} \subset H$.

Suppose $H \neq h\mathbb{Z}$. Therefore, there is an element $x \in H$, such that $x \notin h\mathbb{Z}$. Therefore, by Euclid's Algorithm, there is an integer q such that $nh < x < (n+1)h$; namely, q the quotient of x when evenly divided by h. Therefore, $0 < x - qh < h$.

However, $qh, x \in S$ implies that $x - qh \in H$. This is a contradition, because we have found a positive ineger smaller than h (the smallest positive element of H), which is also an element of H.

Therefore, $H = h\mathbb{Z}$, with $H \in \mathbb{Z}_{\geq 0}$, are all the subgroups of G.

Let us see some applications of Problem 4.1.

Given $a, b \in \mathbb{Z}$, consider $S = a\mathbb{Z} + b\mathbb{Z} = \{n \in \mathbb{Z} : n = ra + sb, r, s \in \mathbb{Z}\}$. Verify that S is a subgroup of $\mathbb{Z}$. Using Problem 4.1, we have that $S = d\mathbb{Z}$, for some integer d.

5 Cyclic Groups (September 18, 2020)

Recall that every subgroup S of $(\mathbb{Z}, +)$ is of the form $d\mathbb{Z}$, for some integer d.

Also, if a, b are integers, we can consider $S = a\mathbb{Z} + b\mathbb{Z}$, which is a subgroup of $\mathbb{Z}$. Therefore, $S\mathbb{Z} = d\mathbb{Z}$. for some integer d.

Since $a, b \in S = a\mathbb{Z} + b\mathbb{Z}$, then $a, b \in d\mathbb{Z}$, which means that d is a divisor of both a, b.

Now, let $n \in \mathbb{Z}$ such that n divides both a and b. Thus, n divides any number of the form $sa + rb$. But, $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, which means $d = ra + bs$, for right choices of r and s. Therefore, n divides d.

Definition 5.1

For $a, b \in \mathbb{Z}$, we define d as above as the *greatest common divisor* of a and b, which we denote by $\gcd(a, b)$.

We have shown not only that d is the greatest common divisor of a and b, but also that any other common divisor of a and b divides d.

Algorithm 5.2 (Euclidean Algorithm)

Example 5.1

Let $a = 314$ and $b = 136$. We divide 314 by 136 and get $314 = 2 \cdot 136 + 42$. Thus,

$$\begin{aligned} n \in 314\mathbb{Z} + 136\mathbb{Z} &\iff n = r \cdot 314 + s \cdot 136 \\ &\iff n = r \cdot (2 \cdot 136 + 402) + s \cdot 136 \\ &\iff n = r \cdot (2r + s) \cdot 136 + r \cdot 42 \\ &\iff n \in 136\mathbb{Z} + 42\mathbb{Z}. \end{aligned}$$

Therefore, $\gcd(314, 136) = \gcd(136, 42)$. We can further use

Definition 5.3

Given $a, b \in \mathbb{Z}$, $a, b \neq 0$, then a and b are relatively prime if, and only if, $\gcd(a, b) = 1$.

Proposition 5.4

The $\gcd(a, b)$ is the product of the prime powers common to prime factorizations of a and b.

Example 5.2

Let $a = 52 = 2^2 \cdot 13$, and $b = 2^3 \cdot 3$. Therefore, $\gcd(52, 24) = 2^2$.

Corollary 5.5

If a and b are relatively prime if, and only if, there are integers r and s such that $ra + sb = 1$.

Corollary 5.6

Suppose p is a prime. Then, given $a, b \in \mathbb{Z}$, if p divides ab, therefore p divides a or p divides b.

Proof. If p divides a, we are done.

Suppose that p does not divide a. Thus, $\gcd(p, a) = 1$. It implies that

$$1 = rp + sa,$$

for some integers r and s. If we multiply both sides by b, we have

$$b = rbp + sab.$$

Notice that p divides both rbp and sab, therefore, p divides their sum, which is b. □

Theorem 5.7

Let $G = (G, \cdot)$ be a group, let I be a set, and let $\{H_i\}_{i \in I}$ be a family of subgroups of G indexed by I. Then, the set

$$\bigcap_{i \in I} H_i$$

is a group.

Proof. We want to show:

(i) $\bigcap_{i \in I} H_i \neq \varnothing$.
For this item, $e \in \bigcap_{i=I} H_i$.

(ii) $a, b \in \bigcap_{i \in I} H_i \implies ab \in \bigcap_{i \in I}$.
For this item, $a, b \in H_i$, for all $i \in I$, which implies $ab \in H_i$ for all i

□

Back to $(\mathbb{Z}, +)$. Given $a, b \in \mathbb{Z}$, let $S = a\mathbb{Z} \cap b\mathbb{Z}$. By the last theorem, S is a subgroup. By Wednesday's theorem, $S = a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$, for some $m \in \mathbb{Z}$. Since $m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, m is a multiple of a and b.

Now, for any number n that is multiple of both a and $b \implies n \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \implies n$ is a multuple of m.

Definition 5.8

The m described above is called the *lowest common multiple* of a and b, denoted by $\text{lcm}(a, b)$.

We have proved above only only that m is the lowest common multiple, but also that m divides every common multiple of a and b.

Definition 5.9

Let $(G, \cdot)$ be a group and $x \in G$. Then the cyclic subgroup generated by x, denoted by $< x >$, is all powers of x, i.e.,

$$\langle x \rangle = \{\dots, x^{-1}, e, x^1, x^2, \dots\}.$$

Theorem 5.10

In G, let $\Gamma(x) = \{H \subseteq G : H \text{ is a subgroup of } G \text{ and } x \in H\}$. Then

$$\bigcap_{H \in \Gamma(x)} H = \langle x \rangle .$$

6 Isomorphisms (September 21, 2020)

This class happened during IMO. The lecture notes are to do.

7 Cosets (September 23, 2020)

This class happened during IMO. The lecture notes are to do.

8 Coset Properties (September 25, 2020)

Definition 8.1 (Equivalence Relation)

An *equivalence relation* is a relation on a set S, i.e., a way to say that certain pairs of elements can be in relationship to one another; so long as the pair satisfies whatever rules we choose for that relationship, AND our rules need to satisfy these properties.

(i) $x \sim x$;
(ii) if $x \sim y$, then $y \sim x$;
(iii) if $x \sim y$ and $y \sim z$, then $x \sim z$.

Remark. If a pair (x, y) satisfy our rules, we write $x \sim y$, "x is equivalent to y".

Definition 8.2 (Equivalence Class)

Given a set S, $s \in S$, and an equivalence relation $\sim$, the *equivalence class of* x, denoted $[x]$, is $[x] = \{y \in S : x \sim y\}$.

Example 8.1

Let $S = \mathbb{Z} \times (\mathbb{Z} - \{0\})$, and we will say that $(a, b) \sim (c, d) \iff ad = bc$. Let us check if the three properties are ensured:

(i) $(a, b) \sim (a, b)$, because $ab = ba$;
(ii) $(a, b) \sim (c, d) \iff ad = bc \iff cb = da \iff (c, d) \sim (a, b)$;
(iii) If $(a, b) \sim (c, d)$ and $(c, d) \sim (r, s)$. Then, $ad = bc$ and $cs = dr$. Therefore, $adcs = bcdr$, which means that $as = br$ (since $c \neq 0 \neq d$). In other words, $(a, b) \sim (r, r)$.

In this case, $[(a, b)] = \{(c, d) \in S : ad = bc\}$.

Theorem 8.3

If S is a set, with an equivalence relation $\sim$, then the equivalence classes of $\sim$ *disjointly partition* S, i.e., every element of S is contained in **exactly** one equivalence class.

Given S, equipped with an equivalence class $\sim$ on S, we define $\bar{S} = \{[x] : x \in S\}$, i.e., the set of equivalence classes.

In this situation, there exists a map $\pi : S \to \bar{S}$, defined by $x \mapsto [x]$.

Example 8.2

Let $S = \mathbb{Z}$, and $a \sim b \iff a - b$ is a multiple of 5. (You should verify that this is an equivalence relation.)

Then $\bar{S} = \{[0], [1], [2], [3], [4]\}$. E.g., $\pi(7) = [2]$.

Definition 8.4

Let $H \leq G$ be groups, and $a \in G$. Then, *the right coset of* H *with respect to* a *is*

$$Ha = \{g \in G : \exists h \in H \text{ such that } ha = g\} = \{ha : h \in H\}.$$

Lemma 8.5

$$Ha = Hb \iff ab^{-1} \in H$$

Lemma 8.6

Given $H \leq G$ groups, the relation defined by $a \sim b \iff ab^{-1} \in H$ is an equivalence relation.

So, what are the equivalence classes of this equivalence relation? They are exactly the right cossets of H, i.e, $[a] = Ha$.

Therefore, right cosets, if distinct, share no elements in common.

On Monday, we'll prove the following theorem.

Theorem 8.7 (Lagrange's Theorem)
If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

9 Normal Subgroups (September 28, 2020)

Lemma 9.1

Given $H \leq G$, if $|G| < \infty$, then given $a, b \in G$, it holds $\#(Ha) = \#(Hb)$.

Proof. Note that H is a right coset ($H = He$). So, suffices to show that for all $a \in G$, $\#(Ha) = |H|$. Define a function $\varphi : H \to Ha$, defined by $h \mapsto ha$. We shall prove that φ is a bijection.

Let's show that φ is onto. Given $g \in Ha$, then $g = ha$ for some $h \in H$. But $\phi(h) = ha = g$, which means that $g \in \text{Im}(\varphi)$.

Let's show that φ is one-to-one. If $\varphi(h_1) = \varphi(h_2) \implies h_1 a = h_2 a = \implies h_1 a a^{-1} = h_2 a a^{-1} \implies a =$

Therefore φ is a bijection, which implies that $\#(Ha) = |H|$, and we're done! □

Theorem 9.2 (Lagrange's Theorem)

If $H \leq G$ are finite groups, then $|H|$ divides $|G|$.

Proof. The right cosets of H partitionate G, i.e., they are disjoint and their union is G; and they all have the same number of elements. Let $[G : H]$ denote the number of right cosets of H sitting inside G, which is called index of H in G. Therefore,

$$G = [G : H] \cdot |H|.$$

□

Corollary 9.3

Given a group G and $a \in G$, if $|G| < \infty$, then order(a) divides $|G|$.

Proof. Consider $\langle a \rangle \leq G$, then, by Lagrange's Theorem, $|\langle a \rangle| = \text{order}(a)$ divides $|G|$ □

Definition 9.4

A subgroup H of G is called *normal*, denoted by $H \lhd G$ if, for all $g \in G$, the image of H under the g-conjugation isomorphism (the g-conjugation isomorphism is the map $\phi_g : G \to G$ defined by $a \mapsto gag^{-1}$) is cointained in H, i.e, $\phi_g(H) \subset H$, for all $g \in G$.

Lemma 9.5

If G and G' are subgroups, $\phi : G \to G'$ a homomorphism, then $\text{Ker}\phi \lhd G$.

Example 9.1

$SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Use Lemma 9.5 with $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$.

Example 9.2

$\langle (1\ 2) \rangle \not\lhd G$, because $\phi_{(2\ 3)}(\langle (1\ 2) \rangle) = \{e, (1\ 3)\} \not\subset H$

Theorem 9.6

The following are equivalent:

(*i*) $H \lhd G$;
(*ii*) $gHg^{-1} = H$, for any $g \in G$;
(*iii*) $gH = Hg$, for any $g \in G$;
(*iv*) Every left coset of H is a right coset of H.

10 Example of Quotients (September 30, 2020)

From last time, we discussed the following theorem:

Theorem 10.1

The following are equivalent:

(*i*) $H \lhd G$;
(*ii*) $gHg^{-1} = H$, for any $g \in G$;
(*iii*) $gH = Hg$, for any $g \in G$;
(*iv*) Every left coset of H is a right coset of H.

Proof (i $\implies$ ii). $H \lhd G \implies \phi_g(H) \in H \implies gHg^{-1} \subset H$. Analougously, $g^{-1}Hg \subset H$. This last one implies that $H \subset gHg^{-1}$.

Therefore, $gHg^{-1} = H$. □

Proof (ii $\iff$ iii). $gHg^{-1} = H \iff gH = Hg$. □

Proof (iii $\implies$ iv). If $gH = Hg$, then gH is a right coset. □

Proof (iv $\implies$ iii). Assume that, given aH, then there is b such that $aH = Hb$. Note that gH sahres an element shares an element (namely, g) with Hg. Since gH is a left coset, then $gH = Hb$ for some b.

Since $g \in gH = Hb$, then Hb intersects with Hg, then $Hb = Hg$ (because, if two left cosets share an element, then they are equal). □

Proof (ii $\implies$ i). $gHg^{-1} = \phi_g(H) = H$, then $\phi_g \subset H$, which implies $H \lhd G$. □

Recall from Linear Algebra:

Theorem 10.2

Let $T : V \to W$ a linear map, then

$$\dim V = \dim \ker T + \dim \operatorname{Im} T.$$

If T is onto, then

$$\dim V = \dim \ker T + \dim W.$$

The goal is to reproduce this idea with groups and homomorphisms, i.e., given G, G' groups, and an onto homomorphism $\phi : G \to G'$, then understand G as being a "stacking" of cosets of $\ker(\phi)$ and when we collapse each coset to a point, we get G'.

Our goal will be realted to the following theorem:

Theorem 10.3

Given G and a subgroup H, then $H \lhd G$ if, and only if, there is a group G' and a homomorphism $\phi : G \to G'$ such that $\ker\ \phi = H$.

Definition 10.4 (Notation)

Let G/H ("G mod H") be the set of all right cosets of H sitting inside G.

Theorem 10.5

When $H \lhd G$, there exists a binary operation on G/H and an homomorphism $\phi : G \to G/H$ such that $\ker\ \phi = H$.

Spoiler: The operation $*$ will be, for $A, B \in G/H$, $A * B = AB = \{g \in G : \exists\ a_1 \in A, b_1 \in B, g = a_1 b_1\}$.

11 Quotient Groups (October 02, 2020)

Here's a rephrasing of our motivation from Linear Alegbra:

Suppose V is a vector space, and $S \subset V$ a subspace. Let $\vec{x} \in V$. In Linear Algebra, we learned we write $\vec{x}$ as a sum of a vector in S with an vector $\vec{z}$ ortogonal to S, a.k.a., $\vec{z} \in S^{\perp}$.

V can be decomposed into parallel copies of S, and there exists a vector space W and a linear map $T : V \to W$ so that T has the effect of collapsing each parallel copy of S to a point. And, ker $T = S$.

To summarize: Given S a subspace of V, there exists a decomposition of V into parallel copies of S and there exists a vector space W and a linear map $T : V \to W$ so that T collapses the parallel copies to points and ker $T = S$.

Our goal in the Group Theory setting: Given $H \lhd G$, there exists a decomposition of G into right cosets of H in G and there exists a group G' and a homomorphism $\phi : G \to G'$ so that ϕ collapses a right cosets of H to a point and $\ker \phi = H$.

On Wednesday, we defined $G/H = \{\text{right cosets of } H \text{ in } G\}$ as our candidate for G'.

Given $Ha, Hb \in G/H$, we defined $Ha * Hb = (Ha)(Hb) = \{h_1 a h_2 b : h_1, h_2 \in H\}$.

We know that $aH = Ha$, then $HaHb = HHab$. Since H is closed under operation and $He = H$, we have that $HH = H$. Thus,

$$Ha * Hb = (Ha)(Hb) = H(ab),$$

which means that $*$ is a binary operation.

So far, we have that G/H has a binary operation. We also have a candidate for ϕ! Define $\phi : G \to G/H$, with $g \to Hg$. Given, $a, b \in G$,

$$\phi(ab) = H(ab) = (Ha)(Hb) = \phi(a)\phi(b),$$

thus ϕ has the homomorphism property. Note also that ϕ is onto.

Lemma 11.1

If G is a group, Y is a set with a binary operation, $\phi : G \to Y$ such that ϕ has the homomorphism property, and ϕ is onto. Then Y is a group and ϕ is a homomorphism.

Proof. We need to show the following items:

(*i*) Assoiativity. Given $a, b, c \in Y$, since ϕ is onto, we have $a = \phi(a'), b = \phi(b'), c = \phi(c')$, for some $a', b', c' \in G$. So

$$\begin{aligned}(ab)c &= (\phi(a')\phi(b'))\phi(c') \\ &= \phi(a'b')\phi(c') \\ &= \phi((a'b')c') \\ &= \phi(a'(b'c')) \\ &= \phi(a')\phi(b'c') \\ &= \phi(a')(\phi(b')\phi(c')) \\ &= a(bc).\end{aligned}$$

(*ii*) Identity. The same strategy as above.
(*iii*) Inverses. The same strategy as above.

Thus, Y is a group. □

12 First Isomorphism Theorem (October 05, 2020)

Summary of our work from last week:

Start with a group G and a normal subgroup H in G. Then, we showed that there exists a way to turn G/H into a group, and, the "natural" map $\phi : G \to G/H$, defined by $g \to Hg$ is an onto homomorphism. The identity of G/H is H. Also, $\ker(\phi) = H$. AND, ϕ has the effect of collapsing each coset of H to a single element.

So, starting with $H \lhd G$, we constructed an onto homomorphism $\phi : G \to G/H$.

Question. If we start with and onto homomorphism $\phi : G \to G'$, when is it the case that ϕ arose via what we did last week?

Theorem 12.1 (1st Isomorphism Theorem)

If $\phi : G \to G'$ is an onto homomorphism, and N denotes $\ker(\phi)$, then G' is isomorphic to G/N.

And, there exists an unique isomorphism $\bar{\phi} : G/n \to G'$ so that $\bar{\phi}$ *commutes* with the natural map $\pi : G \to G/N$, defined by $g \mapsto G/N$, i.e.,

$$\bar{\phi} \circ \pi = \phi.$$

Proof. We want to find a map $\bar{\phi} : G/N \to G$. Let's define

$$\bar{\phi}(Ng) = \phi(g).$$

There is a subtle problem: what if $Ng = Nh$? As we defined $\bar{\phi}$, it sends Ng to $\phi(g)$, and Na to $\phi(a)$. This is a problem unless $\phi(g) = \phi(h)$.

This definition is coherent, because

$$\begin{aligned} Ng = Nh &\implies gh^{-1} \in N = \ker \phi \\ &\implies \phi(gh^{-1}) = e' && (e' \text{ is the identity element of } G') \\ &\implies \phi(g)\phi(h)^{-1} = e' \\ &\implies \phi(g) = \phi(h). \end{aligned}$$

Let's show that $\bar{\phi}$ is a homomorphism:

$$\begin{aligned} \bar{\phi}(NaNb) &= \bar{\phi}(Nab) && (N \text{ is normal}) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) && (\phi \text{ is a homomorphism}) \\ &= \bar{\phi}(Na)\bar{\phi}(Nb). \end{aligned}$$

Let's show that $\bar{\phi}$ is onto: Given $g' \in G'$, there exists $y \in G$ such that $\phi(y) = g'$, since ϕ is onto. So, consider $\pi(y) = Ny \in G/H$. Then, $\bar{\phi}(Ny) = \phi(y) = g'$.

Let's show that $\bar{\phi}$ is one-to-one:

$$\begin{aligned} \bar{\phi}(Na) = \bar{\phi}(Nb) &\implies \phi(a) = \phi(b) \\ &\implies \phi(a)\phi(b)^{-1} = e' \\ &\implies \phi(ab^{-1}) = e' \\ &ab^{-1} \in N \\ &Na = Nb. \end{aligned}$$

Thus, $\bar{\phi}$ satisfies the commuting property! □

13 Example of First Isomorphism Theorem (October 07, 2020)

General idea of today's lecture: 1st iso thm and the conversation about quotient groups from last week are useful for studying a group G from the point of view of onto hom's $\phi : G \to$ something else.

Example 13.1

$G' = \mathbb{Z}^2 = \{(a, b) : a, b \in \mathbb{Z}\}, (a, b) + (c, d) = (a + c, b + d)$. Note: $\mathbb{Z}^2$ is an abelian group (vector addition is commutative).

$G = F_2 =$ "free group on 2 generators" $=$ {finite strings using symbols a, b, a^{-1}, b^{-1}, e}, with the operation of concatenation.

Define $\phi : F_2 \to \mathbb{Z}^2$ by $\phi(a) = (1, 0), \phi(b) = (0, 1)$ and send anything else to where you would have to sent it to make ϕ a homomorphism, e.g., $g \in F_2, g = a^3b^{-2}a^5$; then

$$\begin{aligned}\phi(g) &= 3\phi(a) - 2\phi(b) + 5\phi(a)\\ &= (8, -2).\end{aligned}$$

The function ϕ is onto, since $\phi(a^c b^d) = (c, d)$, for every $(c, d) \in \mathbb{Z}^2$.

Then, by the 1st iso thm, $\mathbb{Z}^2 \simeq F_2/\ker\phi$. (Which implies that, e.g., $F_2/\ker\phi$ is abelian.)

So far, we have that $\mathbb{Z}^2 \simeq F_2/\ker\phi$. So, the idea is: learn something about F_2 by understanding what $\ker\phi$ is. Thus, we want to understand what $\ker\phi$ is.

For example, $aba^{-1}b^{-1} \in \ker\phi$. More generally, if $g_1, g_2 \in F_2$, then $g_1g_2g_1^{-1}g_2^{-1} \in \ker\phi$.

So, $\ker\phi \supset$ group generated by all expressions of the form $g_1g_2g_1^{-1}g_2^{-1}$. It is left to the reader to show that the equality holds. (Think about what it really means for something to be in the kernel.)

Remember, F_2 is not abelian. And a group G is abelian $\iff gh = hg \iff ghg^{-1}h^{-1}$.

The 1st isomorphism theorem says that the elements of $\mathbb{Z}^2$ are representing cosets of $\ker\phi$. This means that $g \in \ker\phi \iff \pi(g) =$ itentity in $F_2/\ker\phi$.

All this to say: $\phi F_2 \to \mathbb{Z}^2$ collapses $\ker\phi$ to a point and collapses each coset of $\ker\phi$ to a different point.

Remember that $\ker\phi = \langle$commutators$\rangle$. The commutators are exactly the stuff that, if they're not identity, the group is not abelian.

So, F_2 is not abelian because $\langle$commutators$\rangle \neq$ {identity element} and we get an abelian group when we quotient out by this subgroup.

In summary:

- We characterized $\ker\phi$ as $\langle$commutators $= g_1g_2g_1^{-1}g_2^{-1}\rangle$ and commutators prevent abelianness. So, $F_2/\ker\phi$ should be abelian. And, 1st iso thm implies $F_2/\ker\phi \simeq \mathbb{Z}^2$, which is abelian.

14 More Examples (October 09, 2020)

Remark. This class has a lot of drawings, which are on Moodle's video of the lecture. The lecture notes for this class are not really useful without the drawings.

Let's show another example of the first isomorphism theorem:

In spirit, the first isomorphism theorem says that if $\phi : G \to G'$ onto, then G is comprised of copies of $\ker \phi$, organized into the pattern of G'.

Example 14.1

Let $G = (\mathbb{Z}, +)$ and $G' = \{0, 1, 2, 3, 4\}$, eqquipped with addition modulo 5. Let $\phi : \mathbb{Z} \to G'$ be the map defined by $k \mapsto k \pmod 5$.

Then, the first isomorphism theorem implies that:

(*i*) $G' \simeq \mathbb{Z}/\ker \phi$.

(*ii*) If $\pi : \mathbb{Z} \to \mathbb{Z}/\ker \phi$ is the natural map defined by $n \mapsto (\ker \phi)n$, then there is an isomorphism $\bar{\phi} : \mathbb{Z}/\ker \phi \to G'$ such that $\phi = \bar{\phi} \circ \pi$.
This implies that, for any $k_1, k_2 \in \mathbb{Z}$, it holds that $\phi(k_1) = \phi(k_2) \iff \pi(k_1) = \pi(k_2)$, i.e., $(\ker \phi) + k_1 = (\ker \phi) + k_2$. (Here, we are using $+$ because that is the group operation.)

SEE THE PICTURES IN THE LECTURE VIDEO.

Example 14.2

Let's apply the same reasoing for $\phi : F_2 \to \mathbb{Z}^2$, from last class.

SEE THE PICTURES IN THE LECTURE.

15 Rings (October 12, 2020)

For groups, our prototype was the *symmetries* of a geometric object.

For rings, our prototypes will be $(\mathbb{Z}, +, \cdot)$, and $(\{f : \mathbb{R} \to \mathbb{R}\}, +, \cdot)$.

Definition 15.1

A ring is a set R, equipped with two binary opperations, $+$ and $\cdot$, satisfying:

(i) $(R, +)$ is an abelian group.
(ii) The operation $\cdot$ is commutative, associative, and has an identity.
(iii) For all $a, b, c \in R$, it holds that $(a + b) \cdot c = a \cdot c + b \cdot c$.

Definition 15.2 (Notations)

We denote $(R, +)$ as R^+. We denote the additive element as 0. We denote the multiplicative element as 1.

Definition 15.3

A subring of a ring R is a subset $S \subset R$, equipped with the same opperations as R.

Subrings of $\mathbb{C}$ were studied as examples of rings in the lecture. The notes for this segment of the class are to do.

16 Units, Fields (October 14, 2020)

Definition 16.1

An element $r \in R$ is called a unit if there exists $s \in R$ such that $rs = 1$.

Lemma 16.2

0 is never a unit, unless R is the trivial group, $\{0\}$.

Definition 16.3

Any non-trivial ring R in which every element except 0 is a unit is called a field.

In other words, a field is a ring in which all non-zero elements have multiplicative inverses.

Example 16.1

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$ (p is prime) are examples of fields.

17 Generalized Evaluation Map (October 16, 2020)

In last class, we learned about the substituion principle. If $\phi : R \to R'$ is a ring homomorphism, and $a \in R'$, then there exists a unique ring homomorphism $\Phi : R[x] \to R'$ satisfying

(*i*) $\Phi|_R = \phi$. (In general, if $f : X \to Y$ and $A \subset X$, we can consider $f|_A : A \to Y$ given by restricting the domain of f to A)
(*ii*) $\Phi(x) = a$.

On Wednesday, we said that "in spirit", this is saying that any ring homomorphism "looks like" a restriction of an evaluation map.

Example 17.1 (Example of Evaluation Map)

Given R a ring and $a \in R$, let $\phi_a : R[x] \to R$ be defined by $p(x) = a_n x^n + \cdots + a_1 x + a_0 \mapsto a_n a^n + \cdots + a_1 a + a_0$. This is an evaluation map, and it is a ring homomorphism

Definition 17.1 (Generalized Evaluation Map)

Assume $\phi : R \to R'$ is a ring homomorphism and fix $a \in R'$. Let $\phi_a : R[x] \to R'$ be defined by

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \mapsto \phi(a_n)a^n + \cdots + \phi(a_1)a + \phi(a_0).$$

Every ring homomorphism $\phi : R \to R'$ is the restriction of a generalized evaluation map from $R[X]$ to R'. And, if we specify $a \in R'$, there is a unique generalized evaluation $\phi_a : R[x] \to R'$ such that ϕ is a restriction of ϕ_a.

Therefore, we can interpret the substitution principle as follows:

Theorem 17.2

Given $\phi : R \to R'$, and $a \in R'$, the generalized evaluation map ϕ_a is a ring homomorphism and it is the only ring homomorphism from $R[x]$ to R' agreeing with ϕ on R and sending x to a.

Let's prove the theorem above (and, consequently, prove the substitution principle).

Proof. We are given $\phi : R \to R'$ and $a \in R'$. We want to show that:

(*i*) The map $\Phi : R[x] \to R'$ defined by $p(x) = a_n x^n + \cdots + a_1 x + a_0 \mapsto \phi(a_n)a^n + \cdots + \phi(a_1)x + \phi(a_0)$ is a ring homomorphism.
(*ii*) It holds that $\Phi|_R = \phi$, and $\Phi(x) = a$.
(*iii*) The map Φ the only ring homomorphism with these properties.

Let's prove each item:

(*i*) We need to show the following items
  (a) $\Phi(1_R) = 1_{R'}$, because $\Phi(1_R) = \phi(1_R) = 1_{R'}$.
  (b) $\Phi(f + g) = \Phi(f) + \Phi(g)$. This item is left to the reader.*

*Use the definition of Φ and use that ϕ is a ring homomorphism.

(c) $\Phi(fg) = \Phi(f)\Phi(g)$. Let $f = \sum_i a_i x^i$ and $g = \sum_j b_j x^j$. Then,

$$\begin{aligned}
\Phi(fg) &= \Phi\left(\sum_i \sum_j a_i b_j x^{i+j}\right) \\
&= \sum_i \sum_j \phi(a_i b_j) a^{i+j} \\
&= \sum_i \sum_j \phi(a_i)\phi(b_j) a^{i+j} \\
&= \left(\sum_i \phi(a_i) a^i\right)\left(\sum_j \phi(b_j) a^j\right) \\
&= \Phi(f)\Phi(g)
\end{aligned}$$

(*ii*) Exercise left to the reader.
(*iii*) Try it!

□

Theorem 17.3 (Slightly more general version of subprinciple)
If $\phi : R \to R'$ is a ring homomorphism and $\alpha_1, \alpha_2, \ldots \alpha_n \in R'$, then there exists a unique ring homomorphism $\Phi : R[x_1, x_2, \ldots, x_n] \to R'$ satisfying $\Phi \mid_R = \phi$ and $\Phi(x_i) = \alpha_i$.

Theorem 17.4
For any ring R, it holds that $R[x, y] \simeq (R[x])[y]$.

Proof. R is a subring of $R[x]$ and $R[x]$ is a subring of $(R[x])[y]$. Thus, R is a subring of $(R[x])[y]$. Therefore, we have a natural obvious ring homomorphism $\phi : R \to (R[x])[y]$.

The substitution principle for $n = 2$, there exists a ring homomorphism $\Phi : R[x, y] \to (R[x])[y]$, extending ϕ.

$R[x]$ is also a subring of $R[x, y]$. Therefore, we have $\gamma : R[x] \to R[x, y]$. The substitution principle, there exists $\Gamma : (R[x])[y] \to R[x, y]$.

Check that Γ is the inverse of Φ. □

18 Ideals (October 19, 2020)

Our plan is to build up the analog of normal subgroups and quotient groups (kernels of homomorphisms), but for rings.

Definition 18.1

An ideal in a ring $(R, +, \cdot)$ is a non-empty subset $I \subseteq R$, such that

(*i*) I is closed under $+$.
(*ii*) For all $r \in R$ and $s \in I$, then $rs \in I$.

Lemma 18.2

If $\phi : R \to R'$ is a ring homomorphism, then $\ker \phi = \{r \in R \mid \phi(r) = 0_{R'}\}$ is an ideal of R.

Proof. Left to the reader. (It is straightfoward). □

Lemma 18.3

I is an ideal if, and only if $I \neq \varnothing$ and any linear combination $r_1 s_1 + \cdots + r_k s_k$ is in I.

Prove this on your own.

Example 18.1 (*i*) Kernels of ring homomorphisms.
(*ii*) (Principal ideal generated by a) If $a \in R$, then $\{ra \mid r \in R\}$ forms an ideal. We write (a) to refer to this ideal.
(*iii*) More generally, given $a_1, \ldots, a_n$, the ideal denoted by $(a_1, \ldots, a_n)$ is $\{a_1 r_1 + \cdots a_n r_n\}$ is an ideal.

Definition 18.4

A proper ideal of R is an ideal of R that is not $\{O_R\}$ nor R.

Lemma 18.5

A proper ideal is never a subring.

Example 18.2

Let $\phi : \mathbb{R}[x] \to \mathbb{R}$ given by $\phi(p(x)) = p(17)$. Then, by the lemma, $\ker \phi$ is an ideal in $\mathbb{R}[x]$.

$$\begin{aligned} \ker \phi &= \{p \in \mathbb{R}[x] \mid p(17) = 0\} \\ &= \{f(x)(x - 17) \mid f \in \mathbb{R}[x]\} \\ &= (x - 17). \end{aligned}$$

Proposition 18.6

If F is a field, then any ideal in $F[x]$ is principal.

Algorithm 18.7 (Polynomial division)

Given $g \in R[x]$ and $f \in R[x]$ monic, there are unique polynomials $p, r \in R[x]$ such that $g = fp + r$, and $\deg(r) < \deg(f)$.

Definition 18.8

If R is a ring and every ideal of R is principal, then it is called a principal ideal domain.

Proposition 18.9 (Rewrite of Proposition 18.6)

If F is a field, then $F[x]$ is a principal ideal domain.

Proof (of Proposition 18.6). Assume that $I \neq \{0\}$. Pick $f(x) \in I$ such that $f(x) \neq 0$ and $\deg(f)$ is minimal. Say that $f(x) = a_n x^n + \cdots + a_0$.

Since F is a field, there is a multiplicative inverse of a_n in F. Thus, let $\tilde{f} = a_n^{-1} \cdot f \in I$, and is monic; also with minimal degree.

Since $\tilde{f} \in I$, we have $(\tilde{f}) \subseteq I$.

Fix $g \in I$. Then, by polynomial division, there are unique $p, r \in F[x]$, with $\deg(r) < \deg(\tilde{f})$ such that $g = p\tilde{f} + r$. Then, $r \in I$, which implies $r = 0$. Thus, $g = p\tilde{f}$. This means that $I \subseteq (\tilde{f})$.

Therefore, $I = (\tilde{f})$. □

Lemma 18.10

If R is a ring, then there exists only one ring homomorphism $\phi : \mathbb{Z} \to R$.

Proof. Define, $\phi(0) = 0_R$ for $n > 0$, $\phi(n) = 1_R + 1_R + \cdots + 1_R$, where 1_R appears n times, and $\phi(-n) = -\phi(n)$. This is the only ring homomorphism that exists. □

Note that $\mathbb{Z}$ is also a principal ideal domain.

So, let $\phi : \mathbb{Z} \to R$ be the unique ring homomorphism. Then $\ker \phi$ is an ideal in $\mathbb{Z}$, so it's principal.

Definition 18.11

The characteristic of R is the positive integer generating $\ker \phi$. If no such integer exists, then $\ker \phi = \{0\}$; in this case, we'll say that the characteristic is 0.

19 Quotient Rings (October 21, 2020)

On Monday, we proved that the kernel of a ring homomorphism is an ideal. Today, we'll see that every ideal can be seen as the kernel of some ring homomorphism.

Theorem 19.1

There exists a natural way of giving $R/I = \{r + I \mid r \in R\}$ a notion of $+$ and $\cdot$ and making it a ring such that the natural map $\pi : R \to R/I$, defined by $r \mapsto r + I$ is a ring homomorphism with $\ker \phi = I$.

Sketch. By the work that we've already done when studying groups, we can understand R/I as an additive group. Thus, our task builds down to defining a multiplication on R/I.

Let's define

$$(I + a) \cdot (I + b) = (I + a)(I + b) = \{a' + b' \mid a' \in I + a, b' \in I + b\}.$$

Note that

$$\begin{aligned}(I + a) \cdot (I + b) &= (I + a)(I + b) \\ &= II + aI + bI + ab \\ &= I + ab.\end{aligned}$$

It is necessary (and ommited here) checking the ring properties.

The proof that π is a ring homomorphism is also ommited. *(It is similar to the group theory analog.)*

Remark. If we prove $\pi : R \to R/I$ is a ring homomorphism, then $\ker \pi = I$ is immediate, since $\pi(i) = I$, for all $i \in I$, and I is the additive identity in R/I.

Theorem 19.2 (*Forgotten* Correspondence Theorem for Groups)

If $G \to G'$ is an onto group homomorphism, then the map $\psi : \{\text{subgroups of } G \text{ containing } \ker \phi\} \to \{\text{subgroups of } G'\}$ defined by $H \mapsto \phi(H)$ and $H' \hookleftarrow \phi^{-1}(H') = \{g \in G \mid \phi(g) \in H'\}$ is a bijective correspondence.

Also, if H and H' are partners and normal, then $G/H \approx G'/H'$.

Theorem 19.3 (Correspondence Theorem for Rings)

If $R \to R'$ is an onto ring homomorphism, then the map $\psi : \{\text{ideals in } R \text{ containing } \ker \phi\} \to \{\text{ideals in } R'\}$ defined by $I \mapsto \phi(I)$ and $I' \hookleftarrow \phi^{-1}(I') = \{r \in R \mid \phi(r) \in I'\}$ is a bijective correspondence.

Also, if I and I' are partners, then $R/I \approx R'/I'$.

Example 19.1

Let $R = \mathbb{C}[x]$ and the ideal $I = \langle x^2 - 1\rangle$. Determine the ideals of $\mathbb{C}[x]/\langle x^2 - 1\rangle$.

Consider the natural map $\pi : \mathbb{C}[x] \mapsto \mathbb{C}[x]/\langle x^2 - 1\rangle$. The correspondance theorem implies that the ideals of $\mathbb{C}[x]/\langle x^2 - 1\rangle$ are in correspondance with the ideals of $\mathbb{C}[x]$ containing $\ker \pi = \langle x^2 - 1\rangle$.

Given an ideal I of $\mathbb{C}[x]$, remember that I is principal by Proposition 18.6 *($\mathbb{C}$ is a field).*

So, there exists a monic polynomial $f(x) \in \mathbb{C}[x]$ such that $I = \langle f(x)\rangle$. If $I \supset \ker \pi = \langle x^2 - 1\rangle$, then $f(x)$ has to be a factor of $x^2 - 1$.

Therefore, $f(x) = 1$ or $f(x) = x^2 - 1$ or $f(x) = x + 1$ or $f(x) = x - 1$.

By the correspondance theorem, there are only 4 ideals in $\mathbb{C}[x]/\langle x^2 - 1\rangle$. They are $\underbrace{\pi(\langle 1\rangle)}_{\mathbb{C}[x]/\langle x^2-1\rangle}$, $\underbrace{\pi(\langle x^2 - 1\rangle)}_{\{0_{\mathbb{C}[x]/\langle x^2-1\rangle}\}}$, $\pi(\langle x + 1\rangle)$, and $\pi(\langle x - 1\rangle)$.

20 Quotient out by an ideal (October 23, 2020)

The point of today's lecture is to understand that "quotienting out by an ideal" is "imposing relations on the original ring of the form (some elements) $= 0$."

Lemma 20.1

$$R/(a,b) \approx (R/(a))/\pi((b))$$

21 Making rings bigger (October 26, 2020)

Example 21.1

Let $R = (\mathbb{R}, +, \cdot)$. We can define a new symbol, i, defined by the equation $i^2 = -1$. Then we get a new ring

$$\mathbb{R}[i] = \{r_0 + r_1 i + r_2 i^2 + \cdots + r_n i^n \mid r_i \in \mathbb{R}\}.$$

But $i^2 = -1$, thus,

$$\mathbb{R}[i] = \{a + bi \mid a, b \in \mathbb{R}\}.$$

Two observations are:

- $\mathbb{R}[i]$ is "a lot smaller" than expected.
- $\mathbb{R}[i] \approx \mathbb{R}[x]/\langle x^2 + 1\rangle$.

Proposition 21.1

Let R be a ring, let $f \in R[x]$ be a monic polynomial, and let n be $\deg f$. Then the quotient ring $R[x]/\langle f\rangle$ satisfies:

(*i*) If we define α, a new element, so that $f(\alpha) = 0$, then $R[x]/\langle f\rangle$ can be identified with $R[\alpha]$, and, any element $\lambda \in R[\alpha]$ can be uniquely expressed as $\lambda = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$ for some $(r_0, \ldots, r_{n-1})$, i.e., $(1_R, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ acts like a basis for $R[\alpha]$.

(*ii*) elements in $R[\alpha]$ are added just like vector addition.

(*iii*) If $\beta_1, \beta_2 \in R[\alpha]$, let $g_1, g_2 \in R[x]$ such that $g_1(\alpha) = \beta_1$ and $g_2(\alpha) = \beta_2$. Then polynomial division implies that there are polynomials $q(x), r(x)$, with $\deg(r) < n$, such that $g_1 g_2(x) = f(x)q(x) + r(x)$. Then $\beta_1\beta_2 = r(\alpha)$.

How else can we make a ring bigger?

Example 21.2

Let $R = (\mathbb{Z}, +, \cdot)$. Then $\mathbb{Q}$ is called the "field of fractions of $\mathbb{Z}$", which is a field you get by starting with $\mathbb{Z}$ and adding in the multiplicative inverses of everything except 0.

Definition 21.2 (Field of Fractions)

Let R be an integral domain (a ring with no zero-divisors, i.e., $xy = 0$ implies $x = 0$ or $y = 0$). Given $R \times (R - \{0_R\})$, let $\sim$ be an equivalence relation defined by $(a, b)\ (c, d) \iff ad = bc$.

Then the field of fractions of R is the set of equivalence classes of this relation. It has the following notions of addition and multiplication:

(*i*) $(a, b) + (c, d) = (ad + bc, bd)$;

(*ii*) $(a, b)(c, d) = (ac, bd)$.

As always, whenever an object has different representations, it is important to show that the operations are consistent (if I change (a, b) to an equivalent (a', b'), then the result is the same).

22 Creating fields from rings (October 28, 2020)

Given a ring R, how can we use it to create a fielf F?

Philosophically, there are two ways to do this:

(i) add elements to R to create some field F in which R is a subring.
(ii) kill elements of R, e.g., create R/I.

For (i), we can only do that if R does not contain zero-divisors, i.e., if R is an integral domain.

Definition 22.1 (Field of Fractions)

Let R be an integral domain (a ring with no zero-divisors, i.e., $xy = 0$ implies $x = 0$ or $y = 0$). Given $R \times (R - \{0_R\})$, let $\sim$ be an equivalence relation defined by $(a, b)\ (c, d) \iff ad = bc$.

Then the field of fractions of R is the set of equivalence classes of this relation. It has the following notions of addition and multiplication:

(i) $(a, b) + (c, d) = (ad + bc, bd)$;
(ii) $(a, b)(c, d) = (ac, bd)$.

As always, whenever an object has different representations, it is important to show that the operations are consistent (if I change (a, b) to an equivalent (a', b'), then the result is the same).

Problem 22.1

Prove that the set $R \times (R - \{0\})$, equipped with the operations defined above, is a ring.

Example 22.1

For $(\mathbb{Z}, +, \cdot)$, $F(\mathbb{Z}) = \{[(a, b)] : a, b \in \mathbb{Z}\}$. In this case, we have $F(\mathbb{Z}) \approx \mathbb{Q}$.

Note also that in $F(R)$, the additive identity is $[(0, 1)]$, and $(0, 1) \sim (0, a)$ for $a \in R - \{0\}$; and the multiplicative identity is $[(1, 1)]$.

So, to show that $F(R)$ is a field, it suffices to show that $[(a, b)]$, where $a \neq 0$, has a multiplicative inverse. If $a \neq 0$, then $[(b, a)] \in F(R)$ and $[(a, b)] \times [(b, a)] = [(ab, ba)] = [(1, 1)]$.

Notationally, we will often denote $[(a, b)]$ as $\frac{a}{b}$.

Proposition 22.2

$F(R)$ is the "smallest" field containing R.

Theorem 22.3 (Mapping principle)

If F_1 is a field, R is an integral domain and $R \subset F_1$, then there is a ring homomorphism $\phi : F(R) \to F_1$. Namely, ϕ maps $\frac{a}{b}$ to ab^{-1}.

Proposition 22.4

The map $\psi : R \to F(R)$, defined by $r \mapsto [(r, 1)]$ is one-to-one.

Before moving to (ii), let's introduce some terminology.

- R is a ring (not necessarily an integral domain).
- $u \in R$ is a *unit* if it has a multiplicative inverse.
- a *divides* b, written as $a \mid b$, if there is $q \in R$ such that $b = aq$.
- a is a *proper divisor* of b if a is not a unit and there is $q \in R$, q is not a unit and $b = aq$.
- a and b are *associates* if each divides each other.
- a is *irreductible* if a does not have proper divisors.
- a is *prime* if it holds that $a \mid bc \implies a \mid b$ or $a \mid c$.

Lemma 22.5

- u is a unit if, and only if, $(u) = R$.
- $a \mid b \iff (b) \subset (a)$.
- a is a proper divisor of b if, and only if, $(b) \subsetneq (a) \subsetneq R$.
- a and b are associates if, and only if, $(a) = (b)$.
- a is irreducible if, and only if, $(a) \subsetneq R$ and there is no $c \in R$ such that $(a) \subsetneq (c) \subsetneq R$.
- a is prime if, and only if, $bc \in (a) \implies b \in (a)$ or $c \in (a)$.

Definition 22.6 (Prime ideal)

A prime ideal I is an ideal such that, if $bc \in I$, then $b \in I$ or $c \in I$.

Definition 22.7

An ideal $I \neq R$ of a ring R is called *maximal* if, whenever J is an ideal and $J \supset I$, then $J = I$ or $J = R$.

In the next class, we will discuss the following theorem:

Theorem 22.8

R/I is a field if, and only if, I is maximal.

Lemma 22.9

A ring R is a field if, and only if, R contains exactly two ideals, namely $\{0\}$ and R.

Proof. If R is a field, then if J is an ideal, suppose $J \neq \{0_R\}$. Then there is some $a \in J$. However, since R is a field, a is a unit. Therefore, $(a) = R$, which implies that $J = R$.

Conversely, for all $a \neq 0$, (a) must be R, thus a is a unit. □

23 Review lecture: Maximal Ideals (November 11, 2020)

Let's recall some definitions.

Definition 23.1 (Ring)

A set R, equipped with two operations $+$ and $\cdot$, is a ring if the following conditions are satisfied:

(i) $(R, +)$ is an abelian group.
(ii) The operaion $\cdot$ is commutative, associative and has an identity.
(iii) For all $a, b, c \in R$, it holds that $(a + b) \cdot c = a \cdot c + b \cdot c$.

Example 23.1 (Rings)

$(\mathbb{Z}, +, \cdot)$ and $R[x]$ for any ring R are examples of rings.

Definition 23.2 (Field)

A ring R is a field if every non-zero element is a unit, i.e., if every non-zero element has a multiplicative inverse.

Example 23.2 (Fields)

$(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ are examples of fields.

Definition 23.3 (Ideal in a Ring)

A non-empty subset $I \subset R$ is an ideal in R if the following conditions are satisfied:

(i) I is closed under $+$.
(ii) For all $r \in R$ and $s \in I$, it holds $rs \in I$.

Example 23.3 (Ideal)

The set of the multiples of 7 is an ideal in $(\mathbb{Z}, +, \cdot)$.

Definition 23.4 (Maximal Ideal)

An ideal I in R is a maximal ideal in R if:

(i) $I \neq R$
(ii) There is no ideal I' in R such that $I \subsetneq I' \subsetneq R$.

Example 23.4 (Maximal Ideals)

The maximal ideals of $\mathbb{Z}$ are the principal ideals generated by prime numbers, $\langle p \rangle$.

The following two propositions will help us to understand how to transform a ring R into a field by removing some of its elements.

Proposition 23.5

Let $\phi : R \to R'$ be a surjective ring homomorphism and let $I = \ker \phi$. *(Remember: the* $\ker \phi$ *of a ring homomorphism is always an ideal.)*

R' is a field if, and only if, I is a maximal ideal.

Proof. From Lemma 22.9, a ring is a field if, and only if, it contains precisely two ideals, itself and 0.

The correspondance theorem says that, for any onto ring homomorphism $\phi : R \to R'$, there exists a bijective correspondence between $\{\text{ideals in } R \text{ containing } \ker \phi\} \leftrightarrow \{\text{ideals in } R'\}$. This bijective correspondance is given by $I \mapsto \phi(I)$ and $\phi^{-1}(I) \hookleftarrow I$.

So, if $I = \ker \phi$ is a maximal ideal, all ideals in R containing I are I and R; which, by the correspondance theorem, implies that R' contains precisely two ideals $\implies$ R' is a ring.

Conversely, if R' is a field, it contains precisely two ideals. Using the correspondance theorem, we have that there are only two ideals in R that contain I. Since I and R are ideals that contain I, they are all of the ideals containing I. This means that there can't be an I' such that $I \subsetneq I' \subsetneq R$, which implies that I is a maximal ideal. □

Corollary 23.6

I is maximal if, and only if, R/I is a field.

Proof. Consider the natural ring homomorphism $\pi : R \to R/I$, given by $r \mapsto r + I$. The kernel of π is I. Therefore, by Proposition 23.5, we have that R/I is a field if, and only if, I is maximal. □

Corollary 23.7

The zero ideal $\{0_R\}$ of R is maximal if, and only if, R is a field.

Proof. Plug in $I = \{0_R\}$ in Corollary 23.6, and we're done. □

Example 23.5 (Transforming $\mathbb{Z}$ into a field by killing elements)

Since $\langle p \rangle = p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, we conclude that $\mathbb{Z}/p\mathbb{Z}$ must be a field.

24 Polynomials (November 13, 2020)

Let's recall some definitions.

Definition 24.1 (Irreductible and Prime Elements)

If R is a ring, a non-unit element $r \in R$ is called *irreductible* if there are no $x, y \in R$, neither of which are units (i.e., neither x nor y have multiplicative inverses) such that $r = xy$.

Also, a non-unit element $s \in R$ is called *prime* if, whenever $s \mid xy$, it holds that $s \mid x$ or $s \mid y$.

Problem 24.1

Let $f \in \mathbb{Z}[x]$. Suppose that f is reducible in $\mathbb{Q}[x]$. Is f reducible in $\mathbb{Z}[x]$?

Lemma 24.2

If $r(x) = b_1 x + b_0 \in \mathbb{Z}[x]$ divides $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, then $b_1 \mid a_n$ and $b_0 \mid a_0$.

Proof. Since $r(x) \mid f(x)$, there exists $q(x) = q_m x^m + \cdots + q_0 \in \mathbb{Z}[x]$ such that

$$a_n x^n + \cdots + a_0 = (b_1 x + b_0)(q_m x^m + \cdots + q_0).$$

By comparing the leading and constant coefficients, we conclude that $a_n = q_m b_1$ and $a_0 = q_0 b_0$, thus $b_1 \mid a_n$ and $b_0 \mid a_0$. □

Lemma 24.3

Assume $b_1 \neq 0$ and $\gcd(b_0, b_1) = 1$. Then $r(x) = b_1 x + b_0 \in \mathbb{Z}[x]$ divides $f \in \mathbb{Z}[x]$ if, and only if, $-\frac{b_0}{b_1}$ is a root of f.

Lemma 24.4

A rational root of a monic polynomial in $\mathbb{Z}[x]$ is an integer.

Proof. Suppose $\frac{p}{q}$ is a root of monic $f \in \mathbb{Z}[x]$. By Lemma 24.3, $qx - p$ divides f. By Lemma 24.2, q divides 1 (the leading coefficient of f). Thus, $\frac{p}{q}$ is an integer. □

Definition 24.5 (Primitive Polynomials)

A polynomial $f(x) = a_n x^n + \cdots + a_0$ is *primitive* if $a_n > 0$ and $\gcd(a_n, \cdots, a_0) = 1$.

Lemma 24.6

Let $f \in \mathbb{Z}[x]$, $\deg(f) > 0$, and $a_n > 0$. Then, the following are equivalent:

(*i*) f is primitive.
(*ii*) For all prime numbers $p \in \mathbb{Z}$, p does not divide f as elements of $\mathbb{Z}[x]$.
(*iii*) If $\psi_p : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ given by mod p on each coefficient, then $f \notin \ker \psi_p$ for all primes p.

Proof.

(*i*) $\implies$ (*ii*): Assume f is primitive $\implies \gcd(a_n, \cdots, a_0)$.
If a prime p would divide f, that would mean that there was a $q(x) = q_m x^m + \cdots + q_0$ such that $f(x) = p \cdot q(x)$. Thus,

$$f(x) = pq_m x^m + \cdots pq_0.$$

Therefore, p divides each coefficients of f, which means $\gcd(a_n, \cdots, a_0) > 1$, a contradiction.

$(ii) \implies (iii)$ Suppose f is not divisible by any prime p. Then, for any p, there is at least one coefficient of f that is not multiple of p. Therefore, f cannot be mapped by ψ_p to the zero polynomial in $\mathbb{Z}/p\mathbb{Z}$, i.e., $f \notin \ker \psi_p$.

$(iii) \implies (i)$ Left as exercise.

□

Proposition 24.7

$\mathbb{Z}[x]$ is an integral domain.

Proof. $\mathbb{Z}[x]$ is an integral domain, because, for all non-zero $f(x) = a_0 + \cdots + a_n x^n, g(x) = b_0 + \cdots + b_m x^m \in \mathbb{Z}[x]$, with $a_n, b_m \neq 0$, the coefficient of x^{m+n} in $(fg)(x)$ is $a_n b_m \neq 0$; thus $fg \neq 0$. □

Proposition 24.8

Let R be an integal domain. If $f \in R$ is prime, then it is irreducible.

Proof. Suppose that $f \in R$ is prime and reducible, i.e., $f = ab$, for some non-units $a, b \in R$.

Since f is prime, f divides a or f divides b. Without loss of generality, assume that f divides a. Thus, we can write $a = fc$, for some $c \in R$. Therefore, it holds that

$$f = fcb.$$

Since R is an integral domain, we can cancel f. Thus,

$$1_R = cb.$$

This implies that b is a unit in R, a contradiction. □

Corollary 24.9

If $f(x) \in \mathbb{Z}[x]$ is prime, then it is irreducible.

25 Gauss' Lemma (November 16, 2020)

We'll continue what we were doing in the last class.

Proposition 25.1

$n \in \mathbb{Z}$ is a prime as a polynomial in $\mathbb{Z}[x]$, i.e., if n is a factor of $p(x)q(x)$, then n divides $p(x)$ or n divides $q(x)$, if, and only if, n is a prime in $\mathbb{Z}$.

Proof. Suppose $n \in \mathbb{Z}$ is prime in $\mathbb{Z}[x]$. By Corollary 24.9, n is irreductible in $\mathbb{Z}[x]$: there are no $a, b \in \mathbb{Z}[x]$ such that $n = ab$ and neither a nor b is ± 1. In particular, there are no $a, b \in \mathbb{Z}$ such that $n = ab$ $(a, b \neq \pm 1)$, which is the usual definition of a prime in $\mathbb{Z}$.

Conversely, suppose taht n is prime in $\mathbb{Z}$. Suppose that $n \mid fg$, for some $f, g \in \mathbb{Z}[x]$. To show that n is prime in $\mathbb{Z}[x]$, we need to show that $n \mid f$ or $n \mid g$.

Let $\phi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the natural ring homomorphism between $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ and let $\psi_n : \mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$ be the ring homomorphism defined by taking ϕ_n on each coefficient. Note that, since n is prime $\implies$ $\mathbb{Z}/n\mathbb{Z}$ is a field $\implies$ $(\mathbb{Z}/n\mathbb{Z})[x]$ is an integral domain.

$$\begin{aligned}
n \mid fg &\iff \psi_n(fg) = 0 \\
&\iff \psi_n(f)\psi_n(g) = 0 && (\psi_n \text{ is a ring homomorphism.}) \\
&\iff \psi_n(f) = 0 \text{ or } \psi_n(g) = 0 && (\mathbb{Z}/n\mathbb{Z}[x] \text{ is an integral domain.}) \\
&\iff n \mid f \text{ or } n \mid g.
\end{aligned}$$

□

Theorem 25.2 (Gauss' Lemma)

The product of primitive polynomails is primitive.

Proof. Let $f, g \in \mathbb{Z}[x]$ be primitive. Then the leading coefficient of fg is the product of the leading coefficients of f and g. Since f, g are primitive, their leading coefficients are positive, which implies that the leading coefficient of fg is also positive.

By Lemma 24.6, for all prime numbers $p \in \mathbb{Z}$, it holds that $p \nmid f$ and $p \nmid g$. By the contrapositive of Proposition 25.1, this implies that $p \nmid fg$, for all prime numbers $p \in \mathbb{Z}$. Again, by Lemma 24.6, we have that fg is primitive. □

Lemma 25.3

Given $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Q}[x]$, there exists a unique way to express $f(x) = c \cdot f_0(x)$, in which $c \in \mathbb{Q}$ and $f_0(x)$ is primitive.

Proof (Existence). Choose $d \in \mathbb{Z}$ such that $d \cdot f \in \mathbb{Z}[x]$, (e.g., choose d to be the lowest common multiple of the denominators of the coefficients of f). Factor out $\pm \gcd(da_0, \cdots, da_n)$ from df (choose $+$ if the leading coefficient of $d \cdot f$ is positive, $-$ otherwise). Thus,

$$f = \pm \frac{\gcd(da_0, \cdots, da_n)}{d} f_0(x).$$

In the equation above $f_0(x)$ is primitive because there is no prime p such that p divides f_0 (if there was, then it would have been factored out "inside the gcd"). □

Proof (Uniqueness). Suppose $f = cf_0 = c'f_0'$, for $c, c' \in \mathbb{Q}$. We can multiply the equation for an apropriate integer (the lowest common multiple of the denominators of c and c') and conclude that, for some relatively prime $d, d' \in \mathbb{Z}$, it holds $df_0 = d'f_0'$.

If $d = d' = 1$, then $f_0 = f_0'$ and $c = c'$, so we're done!

Otherwise, without loss of generality, $d > 0$. Then there exists a prime p such that $p \mid d$. Then, $p \mid df_0 = d'f_0$. Since p is a prime number, by Proposition 25.1, p is a prime as a polynomial in $\mathbb{Z}[x]$. Therefore, $p \mid d'$ or $p \mid f_0'$. The former implies that $p \mid \gcd(d, d') = 1$, a contradiction; and the former implies that f_0' is not primitive, also a contradiction. □

Corollary 25.4

Given $f \in \mathbb{Q}[x]$, write uniquely $f = c \cdot f_0$, with $c \in \mathbb{Q}$ and primitive $f_0 \in \mathbb{Z}[x]$ Then, $f \in \mathbb{Z}[x] \iff c \in \mathbb{Z}$ and $c = \pm \gcd(a_0, a_1, \cdots, a_n)$.

26 Irreducibility over $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ (November 18, 2020)

Theorem 26.1

Let $f_0 \in \mathbb{Z}[x]$ be primitive and $g \in \mathbb{Z}[x]$. Then, if $f_0 \mid g$ in $\mathbb{Q}[x]$, then $f_0 \mid g$ in $\mathbb{Z}[x]$. In other words, if $f_0 h = g$, for some $h \in \mathbb{Q}[x]$, then $h \in \mathbb{Z}[x]$.

Proof. By Lemma 25.3, $h = c \cdot h_0(x)$, in which $c \in \mathbb{Q}$ and $h_0 \in \mathbb{Z}[x]$ is primitive. Therefore,

$$g = f_0 \cdot (c \cdot h_0) = c \cdot (f_0 h_0).$$

Since $f_0 h_0$ is a product of two primitive polynomials, by Gauss' Lemma, $f_0 h_0$ is primitive. Therefore, we have written g as a product of a rational number and a primitive polynomial. Using Corollary 25.4, $g \in \mathbb{Z}[x] \implies c \in \mathbb{Z} \implies h \in \mathbb{Z}[x]$. □

Theorem 26.2

If $f, g \in \mathbb{Z}[x]$ share a common non-constant factor in $\mathbb{Q}[x]$, then f, g also share a common non-constant factor in $\mathbb{Z}[x]$.

Proof. Suppose $h \in \mathbb{Q}[x]$ divides is a factor of f and g. Use Lemma 25.3 to uniquely express $h = c \cdot h_0$, in which $c \in \mathbb{Q}$ and $h_0 \in \mathbb{Z}[x]$ primitive. Since $h \mid f$ and $h \mid g$ in $\mathbb{Q}[x]$, it also holds that $h_0 \mid f$ and $h_0 \mid g$ in $\mathbb{Q}[x]$. By 26.1, $h_0 \mid f$ and $h_0 \mid g$ in $\mathbb{Z}[x]$. □

Theorem 26.3

Let $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}$, with $a_n > 0$. Then:

(*i*) If $\deg(f) > 0$, f is irreducible in $\mathbb{Z}[x]$ if, and only if, f is primitive and irreducible in $\mathbb{Q}[x]$.
(*ii*) If $\deg(f) = 0$, f is irreducible if, and only if, f is a prime number (in $\mathbb{Z}$).

Proof (of i). If f is irreducible in $\mathbb{Q}[x]$, then it is irreducible in $\mathbb{Z}[x]$.

Assume $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$.

If f is not primitive, then $\gcd(a_0, \cdots, a_n) > 1$. This means that we can write f as a product of two non-units as follows

$$f = \gcd(a_0, \ldots, a_n) \cdot f_0,$$

which implies that f is reducible. a contradiction. So, f is primitive.

Assume that there are $g, h \in \mathbb{Q}[x]$ such that $f = gh$. Write $g = c \cdot g_0$ and $h = c' \cdot h_0$, with $c, c' \in \mathbb{Q}$ and $g_0, h_0 \in \mathbb{Z}[x]$ primitive. Therefore,

$$f = (c \cdot g_0)(c' \cdot h_0) = (cc') \cdot (g_0 h_0).$$

By Gauss' Lemma, $g_0 h_0$ is primitive. By Corollary 25.4, $cc' = 1$. Thus,

$$f = g_0 h_0,$$

which means f is reducible in $\mathbb{Z}[x]$, a contradiction. Therefore, f is irreducible in $\mathbb{Q}[x]$. □

Proof (of ii). If f is a constant n, then

$$\begin{aligned} f \text{ is irreducible} &\iff \text{there are no } a, b \in \mathbb{Z}, a, b \neq \pm 1 \text{ such that } n = ab \\ &\iff n \text{ is prime.} \end{aligned}$$

□

Proposition 26.4

Let $f(x) = a_0 + \cdots + a_n x^n$ and p be a prime number. Suppose $p \mid a_n$. Then, if $\psi_p(f)$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$, then f is also irreducible in $\mathbb{Z}[x]$.

Proposition 26.5 (Rational root test)

If $bx - a$ is a factor of $f = c_0 + \cdots + c_n x^n \in \mathbb{Z}[x]$, then $a \mid c_0$ and $b \mid c_n$.

Proposition 26.6 (Degree 2 or 3 test)

If $\deg f = 2$ or 3, then f is reducible in $\mathbb{Q}[x] \implies f$ has a root in $\mathbb{Q}$.

Proposition 26.7 (Eisenstein's criterion)

Let $f(x) = c_0 + \cdots c_n x^n \in \mathbb{Z}[x]$. Suppose there exists a prime p such that $p \nmid c_n$, $p \mid c_{n-1}, \ldots, c_0$, and $p^2 \nmid c_0$. Then, f is irreducible in $\mathbb{Q}[x]$.

27 Field Extensions (November 20, 2020)

Proof (of Eisenstein's Criterion). Suppose $f(x) = c_0 + \cdots + c_n x^n \in \mathbb{Z}[x]$ such that $p \nmid a_n$ and $p \mid a_0, a_1, \ldots, a_{n-1}$. We shall prove that f is reductible in $\mathbb{Q}[x]$implies $p^2 \mid a_0$.

Suppose $f = gh$, with $g, h \in \mathbb{Z}[x]$ and $\deg g, \deg h > 0$. Consider the ring homomorphism $\psi_p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ given by taking each coefficient modulo p. Then,

$$\psi_p(g) \cdot \psi_p(h) = \psi_p(f) = a_n x^n.$$

We claim that $\psi_p(g) = c_r x^r$ and $\psi_p(h) = c_s x^s$.

Suppose $\psi_p(g) = k_r x^r + \cdots + k_{r'} x^{r'}$ and $\psi_p(h) = c_s x^s + \cdots + c_{s'} x^{s'}$, with $k_r, k_{r'}, c_s, c_{s'} \neq 0$ and $r + s = n$. If $r' + s' < n$, then the $(r' + s')^{\text{th}}$ coefficient of $\psi_p(f)$ is $c_{s'} k_{r'}$, but it is also 0, which is an absurd. Therefore, $r' + s' = n \implies r = r'$ and $s = s'$.

Back to $\mathbb{Z}[x]$, g and h have constant coefficients multiples of p, therefore, the constant term of f is multiple of p^2. □

From now on, our focus will be constructing fields and studying their properties and knowing how to tell when a polynomial is irreductible will be extremely helpful.

Definition 27.1 (Field Extension)

If K is a field and $F \subset K$ is a subfield, we say that K is a *field extension of* F and we write K/F.

Example 27.1

A *number field* is any subfield of $\mathbb{C}$, so $\mathbb{C}$ is a field extension of F.

If F is a number field, then $\mathbb{Q} \in F$, because $1 \in F \implies \mathbb{Z} \in F \implies \mathbb{Q} \in F$.

Definition 27.2 (Algebraic Numbers)

Suppose $\alpha \in K$ and K/F. Then, α is *algebraic over* F if there exists a monic polynomial $f \in F[x]$ such taht $f(\alpha) = 0_K$. If α is not algebraic over F, then α is called *transcendental over* F.

Example 27.2

$2\pi i \in \mathbb{C}$ is algebraic over $\mathbb{R}$, since it is a root of $f(x) = x^2 + 4\pi^2 \in \mathbb{Z}[x]$. However, $2\pi i \in \mathbb{C}$ is transcendental over $\mathbb{Q}$.

Example 27.3

If $\alpha \in F$, α is algebraic over F.

Lemma 27.3

Given $\alpha \in K$, K/F. Then α is algebraic over F if, and only if, $\phi_a : F[x] \to K$ is not one-to-one, where $\phi_\alpha(p(x)) = p(\alpha)$.

Proof. ϕ_α is not one-to-one $\iff \ker \phi_\alpha \neq \{0\} \iff$ there exists $F[x], f \neq 0$ and $\phi_\alpha = f(\alpha) = 0 \iff$ there exists a monic polynomial $\tilde{f}$ such that $\tilde{f} = 0$. □

So, suppose $\alpha \in K$ is algebraic over F. Then, $\ker \phi_\alpha \subset F[x]$ is not 0. Recall that the kernel of a ring homomorphism is an ideal, so $\ker \phi_\alpha$ is a non-zero ideal in $F[x]$. Since $F[x]$ is a principal ideal domain, $\ker \phi_\alpha = \langle f(x) \rangle$, for some $f \in F[x]$.

Proposition 27.4

Assume $\alpha \in K$ is algebraic over F. Then, for a given $f \in F[x]$, the following are equivalent:

(*i*) f is the monic polynomial of smallest degree in $F[x]$ such that $f(\alpha) = 0$.
(*ii*) f is irreducible in $F[x]$ and $f(\alpha) = 0$.
(*iii*) $\langle f(x) \rangle = \ker \alpha$ and $\langle f(x) \rangle$ is maximal.
(*iv*) $f(\alpha) = 0$ and if $g \in F[x]$ such that $g(\alpha)$, then $f \mid g$.

Definition 27.5

The polynomial that satisfies Proposition 27.4 is called the *irreducible polynomial for α over F*. The degree of this polynomial is called the *degree of α over F*.

28 More field extensions (November 30, 2020)

General scenarios in which field extensions arise:

(*i*) **"Less abstract":** You have a field K in mind, and an F inside of K. The monic polynomial $f(x) \in F[x]$ is reducible over F and there is a $\alpha \in K$ such that $f(\alpha) = 0$. Then $F(\alpha)$ is the smallest subfield of K containing F and α.
For example, $K = \mathbb{C}$, $F = \mathbb{Q}$, $f(x) = x^2 + 1$, $i \in \mathbb{Q}$ is a root of f; then $\mathbb{Q}(i)$ is a field extension of $\mathbb{Q}$.

(*ii*) **"More abstract":** You have a field F. The monic polynomial $f(x) \in F[x]$ is reducible over F. Then you can invent an abstract element $\alpha \notin K$ and declare it to satisfy $f(\alpha) = 0$. We still can talk about $F(\alpha)$ is the smallest field containing α and F.

I MISSED A SLIDE! ADD IT LATER.

Recall $\phi_\alpha : F[x] \to K$, defined by $p(x) \mapsto p(\alpha)$. The image of this map is $F[\alpha]$. In general, this is a ring. Even more, it is an integral domain.

The field of fractions of $F[\alpha]$ is $F(\alpha)$.

Proposition 28.1

Let $\alpha \in K$, K/F, α algebraic over F, f the monic irreducible polynomial of α over F. Consider $\psi_\alpha : F[x]/\langle f \rangle \to F[\alpha]$, defined by $p(x) + \langle f \rangle \mapsto p(\alpha)$.

Then, ψ_α is an isomorphism.

Proof. Let's recall the ring homomorphism $\phi_\alpha : F[x] \to K$. We can restict the domain to $\Im \phi_\alpha = F[\alpha]$, so that $\phi_\alpha : F[x] \to F[\alpha] \subset K$. This ought to be onto! Thus, by the first isomorphism theorem, $F[x]/\ker \phi_\alpha \approx F[\alpha]$.

However, $\ker \phi_\alpha = \{p \in F[x] \mid p(\alpha) = 0\} = \langle f \rangle$. Thus $F[x]/\langle f \rangle \approx F[\alpha]$.

Recall that the first isomorphism theorem says more than what we've said. It says that there exists an isomorphism $\psi : F[x]/\langle f \rangle \to F[\alpha]$ such that $\psi(\pi(p)) = \phi_\alpha(p)$, where π is the natural map between $F[x] \to F[x]/\langle f \rangle$. This is exact the same ψ_α that we defined in the proposition! □

Corollary 28.2

So, $F[\alpha]$ is a field. (Because $\langle f \rangle$ is maximal.) Therefore, $F[\alpha] = F(\alpha)$.

Proposition 28.3 (11.5.5 from Artin)

$F[\alpha]$ is a vector space over F with basis $(1, \alpha, \ldots, \alpha^{\deg(\alpha)-1})$.

Problem 28.1

Given $\alpha, \beta \in K$, how to tell if $F(\alpha) = F(\beta)$?

29 Quadractic Extensions (December 02, 2020)

Proposition 29.1

Given K/F, K is a vector space over F.

Definition 29.2 (Degree of K/F)

The *degree of* K/F, denoted by $[K : F]$, is the dimension of K as a vector space over F.

Definition 29.3

Some nomenclature:

- K/F is called a finite extensions if $[K : F] < \infty$.
- If $[K : F] = 2$, we call K/F a quadractic extension.
- If $[K : F] = 3$, we call K/F a cubic extension.

Proposition 29.4

K/F satisfies $[K : F] = 1$ if, and only if, $K = F$. Similarly, $\alpha \in K$ has degree 1 over F if, and only if, $\alpha \in F$.

Proposition 29.5

Suppose F is a field with characteristic different than 2, i.e., $1+1 \neq 0$. Suppose K/F and $[K : F] = 2$, i.e., suppose K is a quadratic extension of F. Then, there exists $\delta \in K, \delta \in F$ and $\delta^2 \in F$. In that case, $F(\delta) = K$, and δ "is a square root" of an element of F.

Proof. Since $[K : F] = 2$, there exists some $\alpha \in K, \alpha \notin F$. Therefore, $(1, \alpha)$ are linear independent over F (if one is multiple of the other, than α would be in F). Since the dimension is 2, $(1, \alpha)$ is a basis of K over F.

Consider $\alpha^2 \in K$. It can be written as

$$\alpha^2 = x\alpha + y,$$

for some $x, y \in F$. This implies that

$$\left(\alpha - \frac{x}{1+1}\right)^2 = y - \left(\frac{x}{1+1}\right)^2 \in F.$$

Thus, $\delta = \alpha - \frac{x}{1+1}$ is not in F (if it was in F, then α would be in F.), but $\delta^2 \in F$. Again, for the same reasons, $(1, \delta)$ is a basis of K, which implies $F(\delta) = K$. □

30 Continuing Quadractic Extensions (December 04, 2020)

One question arose: What the heck are we doing?

(*i*) mou learn a lot about a group by understanding its subgroups (especially, the normal subgroups; to use the first isomorphism theorem).
(*ii*) You learn a lot about a group by undestanding its ideals (it's all about the first isomorphism theorem).
(*iii*) You learn a lot about a field by undestanding its subfields (field extensions are useful here).

Continuing:

Theorem 30.1

Let $F \subset K \subset L$ be fields. Then,

$$[L : F] = [L : K][K : F].$$

Proof. Let $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ be a basis for L as a K-vector space; and let $\mathcal{A} = (\alpha_1, \ldots, \alpha_m)$ be a basis for K as a F-vector space. We'll show that $\mathcal{C} = (\alpha_i\beta_j)$ is a basis for L as a F-vector space.

(*i*) $(\alpha_i\beta_j)$ is a spanning set for L over F.
Let $\ell \in L$. Write ℓ as a linear combination of β_j with coefficients in K.
For each coefficient in K, write it as a linear combination of α_i with coefficients in F.
Then, we have expressed ℓ as a linear combination of $\alpha_i\beta_j$ with coefficients in F.
(*ii*) $(\alpha_i\beta_j)$ are linearly independent over F.
Assume there is a linear combination of $\alpha_i\beta_j$ with coefficients in F that sums to 0.
Thus, we can see this as a linar combination of β_j with coefficients in K that sums to 0.
Since $\mathcal{B}$ is linearly independent, each coefficient (which are in K) must be 0.
Note that those coefficients in K are themselves linear combinations of α_i with coefficients in F.
Since $\mathcal{A}$ is linearly independent, those coefficients in F must all be 0.
Therefore, $\mathcal{C}$ is linearly independent over F.

□

31 Corollaries of the Multiplicative Degree Theorem (December 07, 2020)

Let's study some corollaries of the "multiplicative degree theorem" from last class.

Corollary 31.1

Let $F \subset K$ be fields and K/F a finite field extension, in which $[K : F] = n$. Then, for all $\alpha \in K$, α is algebraic over F and $\deg_F(\alpha)$ divides n.

Proof (Algebraic). If α was trancendental, then $F(\alpha)$ is a ∞-dimension vector space over F.

However, since $F(\alpha)$ is a subspace of K, it must have a finite dimension, thus α is algebraic. □

Proof (Division). Using the multiplicative degree formula, we have that

$$[K : F] = [K : F(\alpha)][F(\alpha) : F].$$

Therefore, $\deg_F(\alpha) = [F(\alpha) : F]$ divides $[K : F] = n$. □

Corollary 31.2

Let $F \subset K \subset L$ be fields, and $\alpha \in L$ is algebraic over F. Then, α is algebraic over K and $\deg_K(\alpha) \leq \deg_F(\alpha)$,

Proof (Algebraic). α is algebraic over $F \implies$ there exists a polynomial $f \in F[x]$ with α as a root $\implies$ there exists a polynomial $f \in K[x]$ (namely, the same polynomial) with α as a root $\implies$ α is algebraic over K. □

Corollary 31.3

Let $\alpha_1, \ldots, \alpha_n$ be algebraic over a field F. Then, $[F(\alpha_1, \ldots, \alpha_n) : F] < \infty$.

Sketch. Induction over n.

Corollary 31.4

If K/F is a finite extension, then there are $\alpha_1, \ldots, \alpha_n$ such that $K = F(\alpha_1, \ldots, \alpha_n)$.

Sketch. Let $L_0 = F$.

If $L_i \neq K$, then define $L_{i+1} = L_i(\alpha_{i+1})$, for some $\alpha_{i+1} \in K$ but not in L_i.

This process increases the dimension of $L_\bullet$, but the dimension of $L_\bullet$ may not be greater than the dimension of K. Thus, the process has to terminate, i.e., $F(\alpha_1, \ldots, \alpha_i) = L_i = K$.

Corollary 31.5

If K/F, then the subset of algebraic elements over F is a subfield of K.

Proof. Denote this subset by $\overline{F}$. $1, 0 \in \overline{F}$, since $x, x - 1 \in F[x]$. So $\overline{F}$ is a field if, and only if, given $\alpha, \beta \in \overline{F}$, the elements $\alpha + \beta, \alpha\beta, \alpha^{-1}$ are in $\overline{F}$.

Note that $\alpha + \beta, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)$. Since $F(\alpha, \beta)/F$ is a finite field extension, any element of $F(\alpha, \beta)$ is algebraic over F, which implies that they are on $\overline{F}$. □

Corollary 31.6 (Cor. 15.3.8 on Artin)

Let K/F and K'/F be field extensions. Let L be the field generated by K, K'. If $[K : F]$ and $[K' : F]$ are coprime, then

$$[L : F] = [K : F][K' : F].$$

Sketch. By the multiplicative degree theorem, we have that $[K : F]$ and $[K' : F]$ divide $[L : F]$. Since $[K : F]$ and $[K' : F]$ are coprime, this implies that $[K : F][K' : F]$ divides $[L : F]$.

It suffices to show that $[L : F] \leq [K : F][K' : F]$, i.e., $[L : K] \leq [K' : F]$.

32 (December 9, 2020)

Lecture notes are to do.

33 Finite Fields (December 11, 2020)

A key idea is to note that the natural map $F[x] \to F[x]/\langle f \rangle$ is one-to-one on the constant polynomials, namely F. Thus, in some sense, $F \subset F[x]/\langle f \rangle$.

Lemma 33.1

Let F be a field, and $f(x) \in F[x]$ irreducible over F. Then, in the field $K = F[x]/\langle f \rangle$, the element $\pi(x)$ is a root of f. *(We understand f as being over $F[x]/\langle f \rangle$, since $F \subset F[x]/\langle f \rangle$.)*

Definition 33.2

Let F be a field, and a polynomial $f \in F[x]$ *splits completely* over some field extension K if f factors into linear pieces with coefficients in K.

Lemma 33.3

Given a field F and a monic polynomial f over F, $\deg F > 0$, then there exists a field extension K in which f splits completely.

Sketch. Induction on $\deg f$.

33.1 Finite fields

Theorem 33.4

There exists a field of order p^r, for any prime p and non-negative integer r. Any two fields of order p^r are isomorphic.

Theorem 33.5

If F is a finite field, then $|F| = q$, for some prime p and non-negative integer r.

Theorem 33.6

If $|F| = p^r$, then every element of F is a root of $x^{p^r} - x$.

Theorem 33.7

The irreducible factors of $x^{p^r} - x$ in $\mathbb{Z}/p\mathbb{Z}$ are exactly the irreducible polynomials of $F[x]$, $|F| = p^r$, satisfying the property that their degree divider r.

Theorem 33.8

Let $F^\times$ be the multiplicative group of units in F. It is a cyclic group of order $p^r - 1$.

Theorem 33.9

If $|F| = p^r$, then F has a subfield of order p^k, if $k \mid r$

34 Supplementary Lecture I (December 20, 2020)

The goal today is to prove the following theorem: If K/F is a finite field extension, then there is $\alpha \in K$ such that $K = F(\alpha)$.

First, some background work on polynomials:

Proposition 34.1

Let $f(x), g(x) \in F[x], f(x) \neq 0$ and K/F a field extension.

(a) $F[x]$ is a subring of $K[x]$, so any computation in $F[x]$ is valid in $F[x]$.
(b) Euclidean division of $g(x)$ by $f(x)$ gives the same answer in $F[x]$ or in $K[x]$.
(c) $f(x)$ divides $g(x)$ in $K[x] \iff f(x)$ divides $g(x)$ in $F[x]$.
(d) The monic greatest common denominator, $d(x)$, of $f(x)$ and $g(x)$ is the same, whether computed in $F[x]$ or in $K[x]$.
(e) If $f(x)$ and $g(x)$ have a common root in K, then they are not relatively prime in $F[x]$. Conversely, if $f(x)$ and $g(x)$ are not relatively prime in $F[x]$, there exists an extension of F in which they have a common root.
(f) If $f(x)$ is irreducible over F, and $f(x), g(x)$ have a common root in K, then $f(x)$ divides $g(x)$ in $F[x]$.

Definition 34.2 (Derivative)

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ in $F[x]$, its *derivative* is the polynomial

$$f'(x) = na_n x^{n-1} + (n-1)a_n n - 1x^{n-2} + \cdots + a_1,$$

in which you interpret the integer k as $\underbrace{1_F + 1_F + \cdots + 1_F}_{k \text{ times}}$.

Lemma 34.3

The usual rules of differentiation apply, e.g. product rule.

Lemma 34.4

Let $f(x) \in F[x]$. An element α in an extension K of F is a multiple root, meaning $(x-\alpha)^2$ divides $f(x) \iff \alpha$ is a root of $f'(x)$.

Proposition 34.5

Let $f(x) \in F[x]$. Then there exists a field extension K of F in which $f(x)$ has a multiple root if, and only if, $f(x)$ and $f'(x)$ are not relatively prime.

Lemma 34.6

Let $f(x)$ be a irreducible polynomial over F.

(a) Then, f has no multiple roots in any field extension *unless* $f' = 0$.
(b) In characteristic 0, f has no multiple root over any field extension.

Definition 34.7 (Primitive Element)

Let K/F be a field extension. An element $\alpha \in K$ is called *primitive* if $K = F(\alpha)$.

Theorem 34.8 (Primitive Element Theorem)

Let F be a field of characteristic 0, and let K/F be a finite field extension. Then, there exists a primitive element in K.

35 Supplementary Lecture II (December 25, 2020)

Lemma 35.1

Let F be a field of characteristic 0, and let $K = F(\alpha, \beta)$. Then, for all but finitely many $c \in F$, $\gamma := \alpha + c\beta$ is primitive, i.e., $K = F(\gamma)$.

Proof (of Lemma 35.1). Let $f(x)$ and $g(x)$ be the irreducible polynomials for α, β over F, respectively. There exists a field extension L in which f and g split completely. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m \in K$ be the roots of f and $\beta_1 = \beta, \beta_2, \ldots, \beta_n \in K$ be the roots of g.

Since the characteristic is zero, all α_i's and β_j's are distinct. Let $c \in F$, and let $\gamma_{ij} = \alpha_i + c\beta_j$. There are mn of such γ. Suppose $(i, j) \neq (k, \ell)$. Note that

$$\begin{aligned} \gamma_{ij} = \gamma_{k\ell} &\iff \alpha_i + c\beta_j = \alpha_k + c\beta_\ell \\ &\iff (\beta_j - \beta_\ell)c = \alpha_k - \alpha_i, \end{aligned}$$

which holds for at most one choice of c in F.

Thus, pick some $c \in F$ which is not any of the finitely many elements found above. Then, we have $\gamma_{ij} \neq \gamma_{k\ell}$ for all $(i, j) \neq (k, \ell)$. We shall prove that $\gamma := \gamma_{11} = \alpha_1 + c\beta_1 = \alpha + c\beta$ is primitive. Let $J = F(\gamma)$. Since $\gamma \in K$, we have $J \subset K$. Define a new polynomial, $h(x)$, by

$$h(x) = f(\gamma - cx),$$

which is a polynomial over $F(\gamma)$.

We have shown previously that $\gcd(f(x), h(x))$ is the same when computed in $J[x]$ or in $K[x]$. In $K[x]$, $f(x) = (x - \beta)(x - \beta_2) \cdots (x - \beta_m)$. Since β is a root of $h(x)$, but no $\beta_i, i > 1$, is a root of $h(x)$, we have

$$\gcd(f(x), h(x)) = (x - \beta).$$

Since $f(x), h(x) \in J[x]$, we have that $x - \beta \in J[x] \implies \beta \in J \implies \alpha in J \implies K \subset J \implies K = J$. □

Remark. Since F has characteristic 0, it cannot be a finite field. Thus, there is some c such that

$$F(\alpha + c\beta) = F(\alpha, \beta).$$

Proof (of Theorem 34.8, the Primitive Element Theorem). Since K/F is finite, K is genereated by a finite set, i.e., there exists a finite basis $(\alpha_1, \ldots, \alpha_n)$ for K over F.

Given $\gamma \in K$, there are $a_1, a_2, \ldots, a_n$ such that $\gamma = a_1\alpha_1 + \cdots + a_n\alpha_n$.

Thus,

$$K = F(\alpha_1, \ldots, \alpha_n).$$

Let's induct on n.

- If $n = 1$, then $K = F(\alpha_1)$, so we're done!
- If $n = 2$, then $K = F(\alpha_1, \alpha_2)$. By Lemma 35.1, there exists some γ such that $F(\alpha_1, \alpha_2) = F(\gamma)$, so we're done.
- If $n \geq 3$, then we can use the induction hypothesis on the field $K' = F(\alpha_1, \ldots, \alpha_{n-1})$ and say that K' is generated by a single element. Thus, $K' = F(\beta)$, for some $\beta \in F$. Thus, $K = F(\beta, \alpha_n)$, which is generated by a single element using the base case $n = 2$.

□

36 Splitting fields

Definition 36.1 (Splitting field)

Let F be a field and $f(x) \in F[x]$, not necessarily irreducible over F. There exists some field extension of F such that $f(x)$ splits completely over K, i.e.,

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

The *splitting field of* $f(x)$ *over* F is the field $K = F(\alpha_1, \ldots, \alpha_n)$.

More vaguely, the splitting field of $f(x)$ over F is the smallest (up to isomorphism) field extension of F such that $f(x)$ splits completely.

Proposition 36.2

For every $\beta \in K$, there exists a polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(\alpha_1, \ldots, \alpha_n) = \beta$.

37 Supplementary Lecture III (December 29, 2020)

37.1 Galois Theory

Galois theory presents a way to understand the structure of all subfields of a given field, F, in terms of their "symmetries".

Definition 37.1 (Automorphism and Group of Automorphisms)

An *automorphism* is an isomorphism of a group/ring/field to itself.

Aut($\bullet$) denotes the group of automorphisms of a group/ring/field to itself, under the operation of composition.

Let R be a ring, and $R[u_1, \ldots, u_n]$ be the polynomial ring in n variables.

Given $f \in R[u_1, \ldots, u_n]$, $\sigma \in S_n$, define

$$\sigma(f) = f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}).$$

This new map, from $R[u_1, \ldots, u_n]$ to itself, which we will also denote by σ, is an automorphism of $R[u_1, \ldots, u_n]$.

Definition 37.2 (Symmetric Polynomial)

A *symmetric polynomial* $f \in R[x]$ is one satisfying $\sigma(f) = f$, for all $\sigma \in S_n$.

Proposition 37.3

A polynomial f is symmetric if, and only if, two monomials in the same S_n-orbit, i.e. two monomials such that one can be sent to the other by applying a permutation in S_n, e.g. $u_1u_2^2$ and $u_2u_3^2$, have the same coefficient in g.

Definition 37.4 (Orbit Sum)

An orbit sum is the sum of monomials in a given S_n orbit.

Example 37.1 (Orbit Sum)

One orbit of $R[u_1, u_2, u_3]$ is $\{u_1, u_2, u_3\}$; its orbit sum is $u_1 + u_2 + u_3$.

Another orbit is $\{u_1u_2u_3\}$; its orbit sum is $u_1u_2u_3$.

Proposition 37.5

The symmetric polynomials form a "subspace" [a] of $R[u_1, \ldots, u_n]$ over R. The orbit sums for a basis for this subspace.

[a] This is not a vector space, because R is not a field; but is some sort of analogous when R is a ring.

Definition 37.6 (Elementary Symmetric Polynomials)

The *elementary symmetric polynomials for n variables* are:

$$\begin{aligned} s_1 &= \sum_{i=1}^{n} u_i; \\ s_2 &= \sum_{i<j} u_i u_j; \\ &\vdots \\ s_n &= u_1 u_2 \cdots u_n. \end{aligned}$$

Let $P(x) \in (R[u_1, \ldots, u_n])[x]$ be defined by

$$P(x) = (x - u_1)(x - u_2) \cdots (x - u_n).$$

The coefficients of $P(x)$ are the elementary symmetric polynomials. Explicitely,

$$P(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n.$$

Lemma 37.7 (Girard's Relations)

Suppose f is a monic polynomial in $F[x]$; write it as

$$f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} + \cdots + (-1)^n a_n.$$

Suppose f can be factored (perhaps in a splitting field over F) as $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$. Then,

$$a_i = s_i(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Theorem 37.8 (Symmetric Polynomials Theorem)

Every symmetric polynomial $g(u_1, \ldots, u_n) \in R[u_1, \ldots, u_n]$ can be written in a unique quay as a polynomial in the elementary symmetric polynomials, i.e., there exists a unique polynomial $G(z_1, \ldots, z_n) \in R[z_1, \ldots, z_n]$ such that $g(u_1, \ldots, u_n)$ is obtained by substituting $z_i \mapsto s_i$ in G,

$$g(u_1, \ldots, u_n) = G(s_1, \ldots, s_n).$$

Sketch. Induction on the largest monomial, by lexicographic order on the exponents.

Corollary 37.9

Suppose $f(x) \in F[x]$, and $f(x)$ splits completely over K, with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Let $g(u_1, \ldots, u_n) \in F[u_1, \ldots, u_n]$ be a symmetric polynomial. Then, $g(\alpha_1, \ldots, \alpha_n) \in F$.

Corollary 37.10

Let $p_1(u_1, \ldots, u_n) \in R[u_1, \ldots, u_n]$, and $\{p_1, \ldots, p_k\}$ the S_n-orbit of p_1.[a]

If $h(w_1, \ldots, w_k) \in R[w_1, \ldots, w_k]$ is symmetric, then $h(p_1, \ldots, p_k) \in R[u_1, \ldots, u_n]$ is symmetric.

[a] Note that $k \mid n!$.

Definition 37.11 (Splitting Fields, again)

Let $f \in F[x]$, not necessarily irreducible. A *splitting field* for f is an extension K/F such that

(*i*) f splits completely in K, i.e., $f(x) = (x - \alpha_1)\cdots(x - \alpha_n)$, $\alpha_i \in K$.
(*ii*) $K = F(\alpha_1, \ldots, \alpha_n)$.

Lemma 37.12

Let $F \subset L \subset K$ be fields, and K is a splitting field of $f \in F[x]$. Then, K is a splitting field of f over L.

Lemma 37.13

Every polynomial over F has a splitting field.

Lemma 37.14

A splitting field is a finite extension of F, and every finite extension is contained in a splitting field.

Theorem 37.15 (Splitting Theorem)

Let K/F be a field extension, with K being the splitting field of $f(x)$ over F. Then, if $g(x) \in F[x]$ is irreducible over F and $g(x)$ has at least one root in K, then g splits completely in K.

Proof. Let f, g be as above. We are assuming that there exists $\beta_1 \in K$ such that $g(\beta_1) = 0$. Without loss of generality, g is monic. Since g is irreducible, g is irreducible, g is the minimal polynomial for β_1 over F.

$K = F(\alpha_1, \ldots, \alpha_n)$, with α_i's the roots of f, implies that every element of K can be written as a polynomial in α_i's, with coefficients in F, i.e., there exists $p_1 \in F[u_1, \ldots, u_n]$ such that $p_1(\alpha_1, \ldots, \alpha_n) = \beta_1$.

Let $\{p_1, \ldots, p_k\}$ be the S_n-orbit of p_1.

Let $\beta_j = p_j(\alpha_1, \ldots, \alpha_n)$. So $\beta_1, \ldots, \beta_k \in K$.

Let $h(x) \in K[x]$ be defined by

$$h(x) = (x - \beta_1) \cdots (x - \beta_k).$$

By Corollary 37.10, $s_i(p_1, \ldots, p_k) \in F[u_1, \ldots, u_n]$ is a symmetric polynomial. Then, by Corollary 37.9, $s_i(\beta_1, \ldots, \beta_n) \in F$. Lastly, by Lemma 37.7, the coefficients of $h(x)$ are

$$s_i(\beta_1, \ldots, \beta_k) \in F,$$

which means that $h(x) \in F[x]$.

Therefore, since β_1 is a root of $h(x) \in F[x]$, the irreducible polynomial of β_1, which is g, divides (over F) h, which splits completely over K. This implies that g splits completely K. □