Daily Update

Math 791: Modern Algebra

Spring 2019

Lecture 28: Tuesday, May 9. Thanks, everyone, for a great semester!

We started class by applying Sylow's theorem to prove that a group of order 132 cannot by simple, by considering its various Sylow p-subgroups, the orders of elements in these, and how they overlap one another.

From now on today, we will consider **finite abelian** groups.

Next, we stated and proved the following **lemma**, which allows us to bread down a group into a direct product of subgroups: If G is abelian of order mn, where m and n are relatively prime, then

$$G \cong H \times K$$

where $H = \{x \in G \mid x^m = 1\}$ and $K = \{y \in G \mid y^n = 1\}$. First we proved that H and K are subgroups of G. Then, along with applying Lagrange's theorem and the first isomorphism theorem, we also needed to confirm that $G = HK$ using Bézout's theorem.

By applying this lemma inductively, we obtain the following **corollary**: If $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where the p_i are distinct primes, then

$$G \cong G_1 \times \cdots \times G_r$$

for some groups G_i for which $|G_i| = p^{\alpha_i}$.

From here we stated an **important technical lemma**: If G is abelian of order p^α for p a prime, let $x \in G$ be an element of maximal order among all elements in G. Then for some subgroup H of G,

$$G \cong \langle x \rangle \times H.$$

Applying this inductively, we find that any finite group G of order p^α is the direct product of cyclic groups; i.e.,

$$G \cong Z_{p^{n_1}} \times \cdots \times \times Z_{p^{n_k}}$$

where $n_1 + \cdots + n_k = \alpha$. We saw that the corollary above, with the technical lemma, show that a finite abelian group can be written as a direct product of cyclic groups, each of order some prime, to some power.

Next wrote down three finite abelian groups of order 27, and argued in an ad hoc way that they are distinct. This motivates the full statement of the**Fundamental theorem of finite abelian groups**, which we have already proved a good part of: If G is a finite abelian group, then

$$G \cong Z_{q_1} \times \cdots \times Z_{q_t}$$

where the q_i are powers of (possibly repeated) primes, and this representation is unique up to rearranging the indices.

We used the theorem (and the CRT) to find all finite abelian groups of order 90, and then gave a sketch of the proof of the technical lemma.

Lecture 27: Tuesday, May 7. Throughout class today, p denoted a prime integer. We noticed that for any integer $x > 1$, we can write $x = p^\alpha m$ uniquely, where $\alpha \geq 0$ and $p \nmid m$.

We defined a **p-group** as a group of order p^α for some integer $\alpha \geq 0$. A subgroup H of a group G is called a **p-subgroup** if H is a p-group.

If $|G| = p^\alpha m$ and $p \nmid m$, then if $H \leq G$ and $|H| = p^\alpha$, then H is called a **Sylow p-subgroup** of G. We use $\text{Syl}_p(G)$ to denote the set of all Sylow p-subgroups of G, and $n_p = n_p(G)$ to denote the number of Sylow p-subgroups.

Now we turned to the study of finite groups. First, we recalled that Sylow's theorem ensures a subgroup of order p for any prime p dividing the order of G. Next, we turned to Sylow's theorem, adding on to our preliminary version that we stated earlier:
Sylow's theorem: Suppose that $G = p^\alpha m$, where $p \nmid m$.

1. G has a Sylow p-subgroup; i.e., $\text{Syl}_p(G) \neq \varnothing$.
2. Any two Sylow p-subgroups are conjugate; i.e., given $P, Q \in \text{Syl}_p(G)$, there exists $g \in G$ for which
$$Q = gPg^{-1}.$$
In particular, any two Sylow p-subgroups are isomorphic.
3. $n_p \equiv 1 \bmod p$ and $n_p \mid m$.

We went through some examples of determining Sylow p-subgroups, and verified that the number of them line up with part (3) of the theorem. For example, we noted that if $p \nmid G$, then the unique Sylow p-subgroup is just 1. On the other hand, if $|G| = p^\alpha$, then the unique Sylow p-subgroup of G is G itself. We found all Sylow 2-subgroups and Sylow 2-subgroups of S_3. We also saw that part (3) of the theorem says that for S_4, the number of Sylow 2-subgroups is either 1 or 3, and the number of Sylow 3-subgroups is 1 or 4. As an exercise, investigate which is the case.

We proved that given a Sylow p-subgroup of a group G, then $P \trianglelefteq G$ if and only if $n_p = 1$; i.e., P is the unique Sylow p=subgroup of G.

After this, we turned to applications of Sylow's theorem. In order to describe these, we defined a **simple** group as a group of order at least two, whose only normal subgroups are the trivial group, and the group itself.

We proved that if G has order pq for distinct primes $p < q$, We proved that G is not simple. In particular, it has a unique Sylow q-subgroup, which is normal by our corollary.

Next, we turned to groups G of order p^2q, where p and q are distinct primes. We proved that if $p > q$, then there is a unique Sylow p-subgroup of G, which we know is normal. On the other hand, we proved that if $p < q$, either there is a unique Sylow q-subgroup (which is again normal), or $|G| = 12$. In fact, any group of order 12 has a normal subgroup (check out the example on page 144 of our text), so any group of order p^2q is not simple.

Finally, we saw that $Z_6 \cong Z_2 \times Z_3$, but $Z_4 \ncong Z_2 \times Z_2$. This leads us into our final main theorem, which we will cover next time!

Lecture 26: Thursday, May 2. Today, we covered the **isomorphism theorems for groups**. After reviewing the first isomorphim theorem, given H and K subgroups of a group G, we defined the set $HK = \{hk \mid h \in H, k \in K\}$. We stated the fact that HK is a subgroup of G if and only if $HK = KH$, and proved one direction of this characterization. The other direction was left as a straightforward exercise.

Next, we stated the **second isomorphism theorem for groups**, which we subtitled "a diamond of subgroups:"

Given subgroups A and B of a group G, if $A \leq N_G(B)$, then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and

$$AB/B \cong A/A \cap B.$$

We noticed that the initial conclusions are required to even have that these quotients are themselves groups. After checking these initial conclusions by hand, we finished the proof of this theorem by applying the first isomorphism theorem to the surjective homomorphism $\varphi : A \to AB/B$ given by $\varphi(a) = aB$, whose kernel is $A \cap B$.

Next, we skipped the third isomorphism theorem and turned to the **fourth isomorphism theorem for groups**, subtitled "relating the lattice of subgroups of a group G to that of a quotient group G/N:"

If N is a normal subgroup of a group G, then there is a one-to-one correspondence between subgroups of G containing N, and subgroups of the quotient group G/N. In this bijection, a subgroup A of G containing N corresponds to the subgroup $\overline{A} = A/N$. Moreover,

1. $A \leq B \iff \overline{A} = \overline{B}$
2. $A \leq B \implies |B : A| = |\overline{B} : \overline{A}|$
3. $\overline{A \cap B} = \overline{A} \cap \overline{B}$
4. $A \trianglelefteq G \iff \overline{A} \trianglelefteq \overline{B}$

The proof of each part is straightforward, following through with the definition of cosets.

We gave the beautiful example of the lattice of subgroups of D_8, compared to the lattice of D_8 modulo normal subgroup $\langle r^2 \rangle$.

We returned to cover the **third isomorphism theorem**, and although we did not originally mean to "skip over" it, this was an advantageous in that we saw that the fourth one informs us on this one. We subtitled this theorem "taking quotients of quotient groups," and then sub-subtitled it "invert and cancel:"

Given normal subgroups H and K of a group G, we have that $K/H \trianglelefteq G/H$ and

$$(G/H) \,/\, (K/H) \cong (G/K)$$

i.e., $\overline{G}/\overline{H} \cong G/H$ if the bar denotes the quotient by H.

Finally, we stated the **essential fact** for group homomorphisms induced on quotient groups, an analog of the one we proved for rings: If $\varphi : G \to H$ is a group homomorphism, then for $N \trianglelefteq G$, $\widetilde{\varphi} : G/N \to H$ given by $\widetilde{\varphi}(gH) = \varphi(g)$ is a well-defined group homomorphism if and only if $N \leq \ker \varphi$.

Lecture 25: Tuesday, April 30. We started class by recalling the definition of a **normal subgroup** of a group, and the criterion in which to tell whether two cosets of a group coincide.

We recalled the statement that a subgroup of a group is normal if and only if it is the kernel of some group homomorphism from the group to some other group. We sketched a proof.

Next, we discussed some examples of normal subgroups, pointing out that the trivial group, and the group itself, are normal subgroups of any group. Moreover, any subgroup of an abelian group is normal.

Turning to examples of quotient groups, we proved that finite cyclic group (so abelian) modulo any subgroup is cyclic. We also argued that for any field F and integer $n \geq 1$, $GL_n(F)/SL_n(F) \cong F^\times$.

We showed, by example, that an abelian subgroup of a (non-abelian) group is not necessarily normal. However, if $N \leq G$ and N is a subgroup of the *center* $Z(G)$ of G, then $N \trianglelefteq G$. As an example, we computed the center of D_8 as $Z = \{1.r^2\}$, and computed the four cosets of D_8/Z.

This calculation naturally leads in to **Lagrange's theorem**: If G is a finite group and $H \leq G$, then $|H|\big||G|$ and the number of left cosets of H in G is $|G|/|H|$. As a consequence, if $N \trianglelefteq G$, then $|N/G| = |N|/|G|$. We proved the theorem using the fact that the left cosets partition G. In the proof, we shoed that the number of elements in each coset are the same.

We stated several immediate consequences of Lagrange's theorem. For instance, if $x \in G$ and G is finite, then $|x|\big||G|$, so that in particular, $x^{|G|} = 1$. Moreover, if p is prime and $|G| = p$, then G must be cyclic of order p.

Given H a subgroup of a group (that is not necessarily finite) G. Then the **index** of H in G, denoted $|G : H|$, is the number of left cosets of H in G. Therefore, if G is finite, then $|G : H| = |G|/|H|$, which equals $|G/H|$ if $H \trianglelefteq G$. However, we used the example $\langle n \rangle \subseteq \mathbb{Z}$ to show that if a group G is infinite, then it is not necessarily true that the index of a subgroup in G must be infinite.

Using the theory built to far, we proved that if H is a subgroup of a group G and $|G : H| = 2$, then H is normal in G, and $G/H \cong Z_2$!

We next pointed out that although $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$ (and each subgroup has index 2 in the next group), $\langle s \rangle \not\trianglelefteq D_8$ since $rsr^{-1} = sr^2 \notin \langle s \rangle$.

After this, we stated **Cauchy's theorem**; its proof (§3.2, #9) is group homework: If G is finite and a prime p divides $|G|$, then G has an element of order p. We also stated a *preliminary version* of **Sylow's theorem**: If G is a finite group of order $p^\alpha m$, where p is a prime and $p \nmid m$, then G has a subgroup of order p^α.

Finally, we stated the **First isomorphism theorem for groups**, that has already been proved: If $\varphi : G \to H$ is a group homomorphism, then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \operatorname{Im} \varphi$. As consequences, we know that φ is injective if and only if $\ker \varphi = 1$, and $|G : \ker \varphi| = |\operatorname{Im} \varphi|$.

Be ready for a **quiz on normal subgroups and quotient groups** on Thursday!

Lecture 24: Thursday, April 24. We stated class by defining the **cosets** of a subgroup in a group: If $N \leq G$ and $g \in G$, then we define the **left coset** of g as $gN = \{gn \mid n \in N\}$, and the **right coset** of g as $Ng = \{ng \mid n \in N\}$. Any element of a coset is called a **representative** of the coset.

We can think of the cosets as "translations" of the subgroup by an element of the group. If G has addition as its operation, we write the cosets analogously as $g + N$ and $N + g$. We noticed how this definition serves as an analog of the cosets of a ring modulo an ideal.

We then rewrote the last **proposition** stated last class in terms of cosets: Let $\varphi : G \to H$ be a group homomorphism with kernel K. Moreover, let $X = \varphi^{-1}(a) \in G/K$ for some $a \in H$. Then for any $u \in X$,

$$X = uK = Ku.$$

We prove this proposition, and pointed out that this means that the left cosets of the kernel K of a homomorphism, which are the fibers of the homomorphism, are precisely the elements of G/K. Moreover, the operation we defined on the fibers in G/K is identical to the operation on the cosets

defined by, for $u \in G$,

$$(uK)(vK) = (uv)K.$$

We explicitly went through several examples of quotients G/K, now writing the elements as left cosets. One example was projection from $\mathbb{R}^2$ to $\mathbb{R}$, onto the first coordinate; the cosets are lines $x = 1$, and the operation is given by $(x = 1) + (x = b) = (x = a + b)$.

Now we turned to the following looming **question**: Can we define a quotient group G/N for *any* subgroup N of G?

We started to address this question by studying the cosets of $N \leq G$ in more detail, proving the following:

- The set of left cosets of N in G partition G, so that $uN \neq vN \iff uN \cap vN = \varnothing$.
- $uN = vN \iff v^{-1}u \in N$.
- In particular, $vN = uN \iff v \in uN$.

Finally, we were able to address the question above, proving the following **theorem**: Given a subgroup N of a group G, the operation on left cosets given by

$$uN \cdot vN = (uv)N$$

is well defined if and only if $gng^{-1} \in N$ for all $g \in G$, and all $n \in N$.

We left the following additional (and very important) statement as a straightforward exercise: In the case that the operation is well-defined, the left cosets form a group under this operation, which we call the **quotient/factor group** G/N. In particular, the identity is $N = 1N$ and the inverse of gN for $g \in G$ is $g^{-1}N$.

Finally, we gave the following series of **definitions**: Given N a subgroup of a group G,

- For $g \in G$ and $n \in N$, gng^{-1} is the **conjugate** of n by g.
- For $g \in G$, $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the **conjugate** of N by g.
- We say that g **normalizes** N if $gNg^{-1} = N$.
- N is a **normal subgroup** of G if every element of G normalizes N; i.e., for all $g \in G$,

  $$gNg^{-1} = N$$

  To signify that N is a normal subgroup of G, we write $N \trianglelefteq G$.

  To wrap up our work so far, we noted that **the following are equivalent** for a subgroup N of G:

  1. $N \trianglelefteq G$.
  2. $gNg^{-1} \subseteq N$ for all $g \in G$.
  3. The set of left cosets $\{gN \mid g \in G\}$ of N form a group G/N under the operation $gN \cdot g'N = gg'N$.
  4. The left and right cosets coincide; i.e., $gN = Ng$ for all $g \in G$.
  5. $N_G(N) = G$.

Finally, we related the theory built for quotient groups constructed modulo the kernel of a homomorphism by stating the following fundamental **theorem**: A subgroup N of a group G is normal if and only if N is the kernel of a group homomorphism from G to some group H.

Lecture 23: Tuesday, April 23. We started class today by introducing the notation Z_n for a finite cyclic group of order n under multiplication; from our theory proved last time, we know that $Z_n \cong \mathbb{Z}/n\mathbb{Z}$ where, of course, the latter group has addition as its operation.

Next, we proved the first part of the final theorem stated last time, classifying all subgroups of any cyclic group. We left the second part as homework; please refer to the proof of the third part in the book for hints, if you need a hint (you probably don't!).

After this, we used this theorem, and our theorem classifying all generators of a cyclic group (given one generator), to find all subgroups, and all their generators, of $\mathbb{Z}/12\mathbb{Z}$. We also noticed which subgroups sit inside one another.

Next, we returned to our discussion of group homomorphisms, defining the **kernel** of a group homomorphism $\varphi : G \to H$ as

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}.$$

We stated the following facts about group homomorphisms, and proved parts (1) and (4). In particular, we noticed that things work differently that for ring homomorphisms, so we need to be especially careful, since we are so well-versed in dealing with the ring version!

1. $\varphi(1_g) = 1_H$.
2. For all $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.
3. For all $g \in G$ and $n \in \mathbb{Z}$, $\varphi(g^n) = \varphi(g)^n$.
4. $\ker \varphi \leq G$.
5. $\operatorname{Im} \varphi \leq H$.

From here, we recalled that a *fiber* over $t \in T$ of a function $f : S \to T$ between sets is $f^{-1}(s)$, the set of elements in S mapping to t.

Given a group homomorphism $\varphi : G \to H$, we considered the fibers $X_a := \varphi^{-1}(a)$ over elements $a \in H$, drawing this pictorially. Notice that $X_1 = \varphi^{-1}(1) = \ker \varphi$. After first motivating this heuristically, we proved that the fibers form a group under the following operation induced by the group operation in H: Given $a, b \in H$, we define

$$X_a X_b = X_{ab}.$$

This partitions G into pieces, so that the pieces form a group. We noticed what happens in this setup when φ is an isomorphism, or the trivial homomorphism sending every element to the identity.

We call the new group a **quotient group** or **factor group** modulo the kernel of φ, and denote it G/K, where $K = \ker \varphi$.

We saw very concretely that the quotient group modulo the kernel of the group homomorphism $\varphi : \mathbb{Z} \to Z_n$ given by $a \to x^a$, where x is a generator for Z_n, is equal to $\mathbb{Z}/n/\mathbb{Z}$, which we know, in turn, is isomorphic to Z_n.

Finally, we stated a **proposition** that will help us transition to the study of quotient groups modulo a general subgroup: Given a group homomorphism $\varphi : G \to H$ with kernel K, let $X = \varphi^{-1}(a) \in G/K$ for some element $a \in K$. Then for any $u \in X$,

$$X = \{uk \mid k \in K\} - \{ku \mid k \in K\}.$$

Lecture 22: Thursday, April 18. We started class by recalling the definition of the **centralizer** $C_G(A)$ of a nonempty subset A of a group G, and the **center** of G. We proved both are subgroups of G. For $g \in G$, we then defined the set gAg^{-1} as the set of elements of the form gag^{-1}, for $a \in A$. We then defined the **normalizer** of A in G as

$$N_G(A) = \{g \in G \mid gAg^{-1} - A\}$$

which is also a subgroup of G. We noticed that

$$Z(G) \leq C_G(A) \leq N_G(A) \leq G$$

and that if G is abelian, then $Z(G) = G$, so that every subgroup above must coincide with G.

After this, we carried out a detailed study of **cyclic groups**. We call a group H **cyclic** if it can be generated by one element $x \in H$, i.e.,

$$H = \{x^n \mid n \in \mathbb{Z}\},$$

or using additive notation, $H = \{nx \mid n \in \mathbb{Z}\}$. If H is generated by $x \in H$, then we write $H = \langle x \rangle$.

We gave several examples, showing that ± 1 are generators for $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$, 2 is not a generator of $\mathbb{Z}/4\mathbb{Z}$, and that 2 is a generator for $(\mathbb{Z}/5\mathbb{Z})^\times$, but that $(\mathbb{Z}/8\mathbb{Z})^\times$ is *not* cyclic.

We stated and proved a **proposition**: If $H = \langle x \rangle$, then $|H| = |x|$. Moreover,

1. If $|H| = n < \infty$, then
$$a, x, x^2, \ldots, x^{n-1}$$
are all the (distinct) elements of H.
2. If $|H| = \infty$, then $x^n \neq 1$ for any nonzero integer n, and $x^a \neq x^b$ for all distinct integers a, b.

After this, we stated and proved, using Bézout's theorem, the following **fact**: If x is an element of a group and $x^m = x^n = 1$ for some integers m, n, then $x^d = 1$, where $d = (m, n)$, the greatest common divisor of m and n. In particular (taking $n = |x|$), if $x^m = 1$, then $|x| \mid m$.

After this, we wrapped our work together with the following **theorem**: Any two cyclic groups of the same order are isomorphic. Moreover,

1. If $n \in \mathbb{Z}^+$ and $|\langle x \rangle| = |\langle y \rangle| = n$, then the following is a well-defined isomorphism:
$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$
2. If $\langle x \rangle$ is infinite, then the following is a well-defined isomorphism:
$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

We used this theorem to conclude that any finite cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$: for example, the subgroup of D_{2n} of rotations.

After this, stated a **proposition**: If x is an element of any group and a is an integer, then

1. If $|x| < \infty$, then $|x^a| = \infty$

2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$. In particular, if $a \mid n$, then $|x^a| = \frac{n}{a}$.

We used this to deduce following: Suppose that $H = \langle x \rangle$. Then

1. If $|x| < \infty$, then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.
2. If $|x| = n < \infty$, then $|H| = \langle x^a \rangle$ if and only if $(a, n) = 1$, so that in particular, the number of generators of H is $\varphi(n)$.

We applied this theorem to our examples presented earlier in class.

Finally, we stated the first two parts of the following **theorem** about subgroups of a cyclic group $H = \langle x \rangle$.

1. Every subgroup of H is cyclic, and if $K \leq H$, then $K = \{1\}$ or $K = \langle x^d \rangle$, for d the smallest positive integer for which $x^d \in K$.
2. If $|H| = \infty$ and $a, b \geq 0$, then $\langle x^a \rangle \neq \langle x^b \rangle$, and $\langle x^a \rangle = \langle x^{-a} \rangle$, so that the subgroups of H are in one-to-one correspondence with the nonnegative integers, where $k \leftrightarrow \langle x^k \rangle$.
3. If $|H| = n < \infty$, then for all $a > 0$, $a \mid n$, there exists a unique subgroup of H or order a, $\langle x^d \rangle$, where $d = \frac{n}{a}$, and for all integers m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$. Therefore, the subgroups of H are in one-to-one correspondence with the positive divisors of n.

Lecture 21: Tuesday, April 16. Today, we introduced **symmetric groups**, and did several examples. We also defined certain **matrix groups**; in particular, the **special** and **general linear groups**: If F is a field,

$$SL_n(F) = \{A \in M_n(F) \mid \det(A) = 1\}$$
$$GL_n(F) = \{A \in M_n(F) \mid \det(A) \neq 0\}$$

After this, we defined a **group homomorphism** of groups as a function that preserves the group operations: Given groupgroups, $(G, *)$ and $(H, \diamond)$, $\varphi : G \to H$ is a group homomorphism if for all $g, g' \in G$,

$$\varphi(g * g') = \varphi(g) \diamond \varphi(g').$$

Using our typical multiplication for arbitrary groups, this translates as $\varphi(gg') = \varphi(g)\varphi(g')$.

We say that a group homomorphism is a **group isomorphism** if it bijective, and call the two groups **isomorphic**, writing $G \cong H$.

An example of a group isomorphism is the map $\exp : \mathbb{R} \to \mathbb{R}^+$ (where $\mathbb{R}$ is the additive group, and $\mathbb{R}^+$ is the multiplicative group) given by $\exp(x) = e^x$, so that $e^{x+y} = e^x e^y$.

We noted that if $\varphi : G \to H$ is a group isomorphism, then $|G| = |H|$, G is abelian if and only if H is abelian, and the order of $x \in G$ is the same as the order of $\varphi(x) \in H$.

After this, we defined a **subgroup** H of a group G as a nonempty subset that is closed under taking products and taking inverses. We write $H \leq G$ as shorthand for "H is a subgroup of G."

We gave several examples of subgroups, noting that the set of rotations is a subgroup of the dihedral group, but the set of reflections is not.

We then stated the **subgroup criterion**: a subset H of a group G is a subgroup of G if and only if:

1. $H \neq \varnothing$

2. $xy^{-1} \in H$ for all $x, y \in H$.

Moreover, if $|H| < \infty$, we have a **finite subgroup criterion**: a finite subset H of a group G is a subgroup of G if and only if:

1. $H \neq \varnothing$
2. $xy \in H$ for all $x, y \in H$.

In a group effort, we proved both criteria.

Finally, given a group G and a nonempty subset A of G, the **centralizer** of A in G is

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ consists of all elements in G that commute with every element in A. The **center** $Z(G)$ of G is $C_G(G)$; i.e.,

$$Z(G) = \{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\}.$$

In fact, $Z(G) \leq C_G(A) \leq G$ for all nonempty subsets A of G.

Lecture 20: Tuesday, April 9. We started class by briefly going over some "tricks" for finding minimal polynomials.

Next, we defined a **group** $(G, *)$ as a set G with a binary operation $*$ satisfying the following:

1. *Associativity*: For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
2. *Identity*: There exists an element $e \in G$ for which $e * a = a * e = a$ for every $a \in G$.
3. *Inverses*: Given $a \in G$, there exists $a^{-1} \in G$ for which $a * a^{-1} = a^{-1} * a = e$.

Moreover, we call $(G*)$ **abelian** if it satisfies the *commutative law*: $a * b = b * a$ for all $a, b \in G$.

Instead of writing $(G, *)$, we often say that "G is a group under the operation $*$."

We gave several examples of groups: A ring R is an abelian group under addition, with identity 0 and inverse $-r$ of an element $r \in R$. Thus all of the rings we are familiar with are groups under addition, including $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$, rings of functions, matrix rings, polynomial rings, products of rings, quotient rings, ... In each case, 0 is the identity, and negatives are inverses.

Notice, though, R is *never* a group under multiplication since then $1 \in R$, so that there is an identity, but $1 * 0 = 0 \neq 1$. However, we noticed that we can make some familiar rings into groups under addition by removing 0; e.g., $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$ are all groups under multiplication with identity 1. On the other hand, $(\mathbb{Z} \setminus \{0\}, \cdot)$ *cannot* be a group since, for example, 2 has no inverse. We can fix this by considering the examples above as the sets of *units* of the ring: e.g., $\mathbb{Q}^\times \mathbb{Q} \setminus \{0\}$. In fact, $\mathbb{Z}^\times = \{-1, 1\}$ is also a group under multiplication, and we checked that this is the "same" group as $(\mathbb{Z}/2\mathbb{Z}, +)$.

In fact, we verified that given any ring R with 1, $(R^*, \cdot)$ is a group. We saw what this means for $R = \mathbb{Z}/n\mathbb{Z}$ and $R = M_n(\mathbb{R})$.

After this, we defined the **product** of rings $(G, *)$ and $(H, \star)$: $G \times G$ is defined as the set of coordinate pairs (g, h) for $g \in G$ and $h \in H$, and given $g, g' \in G$ and $h, h' \in H$, we define the operation $\diamond$ as $(g, h) \diamond (g', h') = (g * g', h \star h')$.

We stated a **theorem** that collected several facts about a group $(G, *)$: Its identity is unique, inverses are unique, $(a^{-1})^{-1} = a$ for all $a \in G$, and $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Since the operation $*$ becomes unwieldy, we often use $\cdot$ as the operation for an abstract group (and often omit the symbol in products), 1 for its identity, and (like we have today) a^{-1} for the inverse of an element a of the group.

We stated and showed that **cancellation** holds in groups, and given elements a, b of a group, equations of the form $ax = b$ and $xa = b$ have unique solutions in the group.

Given an element x of a group G, the **order** of x, denoted $|x|$, is the smallest positive integer for which $x^n = 1$, if this number exists. If no such integer exists, we say that the order is infinite.

We went through several examples of finding orders of an element in a group.

After this, we introduced the **dihedral group** D_{2n} of symmetries of a regular n-gon. We did examples with $n = 3$ and $n = 4$, and showed in general that the group D_{2n} has order $2n$. We also defined the elements r and s of D_{2n}, after putting the n-gon in the plane, centered at the origin: r is the rotation clockwise by the angle $2\pi/n$, and s is the reflection about the line passing through the first vertex, and the origin.

Lecture 19: Thursday, April 4. We started class by recalling that a finite field extension is algebraic, but pointed out that although we proved that the converse holds for simple, or even *finitely generated* extensions, it does not hold in general; for instance, consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt[2]{2}, \sqrt[4]{2}, \ldots)$ of $\mathbb{Q}$.

Next, we stated and proved a corollary of the partial converse above: Given a field extension K/F, the set of elements $\overline{F}$ of K that are algebraic over F form a subfield of K. In fact, we call this the **algebraic closure** of F in K. We investigated the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Next, we discussed the fact that if $F \subseteq K \subseteq L$ are fields, and K/F and L/K are both algebraic, then L/F is also algebraic.

After this, we defined what it means for a field extension K of a field F to be a **splitting field** for $f \in F[x]$: f splits completely into linear factors over K, but not over any subfield of K. In fact, there exists a splitting field for any polynomial over a field, and it is unique up to isomorphism.

We went through several examples, finding splitting fields for $x^2 - 2, (x^2 - 2)(x^2 - 3), x^3 - 2, x^2 + 1 \in \mathbb{Q}[x]$. For each, we found the degree of the extension, and it was *not* always the degree of the polynomial. In fact, our proof of existence of the splitting field shows that the degree of the splitting field over the base field is at most $n!$, where $n = \deg(f)$.

After this, we started a discussion on the splitting field of $x^n - 1 \in \mathbb{Q}[x]$, which leads naturally to the notion of the *n-th roots of unity*.

Finally, as our capstone to the field theory in this course, we sketched a proof of the following fundamental theorem: Given any prime integer p and integer $n \geq 1$, there exists a field $\mathbb{F}_{p^n}$ with p^n elements.

Lecture 18: Tuesday, April 2. We started class by pointing out that the last problem on Quiz 6 requires Gauss' lemma (like the first problem on Quiz 7!).

Next, we recalled the notions of *algebraic* and *transcendental*, and discussed some of what is known about real numbers that are algebraic/transcendental over the field of rational numbers.

Again, throughout class today, K/F is a field extension.

We recalled where we left off in the proof of existence of the **minimal polynomial** $m_{\alpha,F}(x) = m_\alpha(x) \in F[x]$ of $\alpha \in K$ over F. Our work essentially finished off the proof, modulo some explanation. Recall that $f \in F[x]$ has α as a root if and only if $m_\alpha \mid f$, and that we call $\deg m_\alpha$ the **degree of** $\alpha \in K$ **over** F, often denoted $\deg \alpha$.

We noted that by our work so far shows that if α is algebraic over F, then

$$F(\alpha) \cong F[x]/(m_\alpha(x))$$

since K is an extension field containing a root of of $m_\alpha(x)$. Moreover,

$$[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha.$$

We went through several basic examples, finding the degrees and/or minimial polynomials: $\sqrt{2} \in \mathbb{R}$ over $\mathbb{Q}$, $\sqrt[3]{2} \in \mathbb{R}$ over $\mathbb{Q}$, $\sqrt[n]{2}$ over $\mathbb{Q}$, the same over $\mathbb{R}$, and the degree of any root of $x^2 - 3x - 1$ over $\mathbb{Q}$.

From here, we turned to some fundamental results on field extensions. We proved that $\alpha \in K$ is algebraic over F if and only if the extension $F(\alpha)/F$ is finite. As a corollary, a finite extension is necessarily algebraic (but the converse need not always hold!).

We gave the basic argument behind the fact that if $F \subseteq K \subseteq L$ are fields, then

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

even if any are infinite. As a corollary, a finite extension of a finite extension is again a finite extension.

We saw the above statement realized for the extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$.

Next, we defined an extension K/F as **finitely generated** if $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in K$. In fact, given $\alpha, \beta \in K$, $F(\alpha, \beta) = (F(\alpha))(\beta)$, and we can "extend" inductively to get a more general statement for finitely generated extensions.

We considered some examples of finitely generated extensions. We saw that $\mathbb{Q}(\sqrt{2}, \sqrt[6]{2}$ is the simple extension $\mathbb{Q}(\sqrt[6]{2}$. and that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ by carefully considering the extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq (\sqrt{2}, \sqrt{3})$.

We stated the following **theorem**: K/F is a finite extension if and only if $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in K$ algebraic. Moreover, $[K : F]$ is bounded above by the product of the $[F(\alpha_i) : F]$. We gave the basic idea behind this.

Finally, we stated and proved a **corollary**: If $\alpha, \beta \in K$ are algebraic over F, then

$$\alpha \pm \beta, \alpha\beta, \text{ and } \frac{\alpha}{\beta}$$

(where the last requires $\beta \neq 0$) are algebraic over F. In particular, the inverse of any algebraic element is again algebraic over F.

Lecture 17: Thursday, March 28. We started class by pointing out some common mistakes on our quiz on determining whether certain polynomials are irreducible. We know that if F is a field and $f \in F$ is a nonzero polynomial, then for $a \in F$,

$$f(a) = 0 \iff (x - a) \mid f.$$

On the other hand, if $g \in R[x]$ for R any commutative ring, we have that if $a \in R$ and $(x-a) \mid g$, then $g = (x-a)h$ for some $h \in R[x]$, so if $\deg g \geq 2$, then g is reducible. However, the converse does

not necessarily hold; for instance, consider $g = x^2 - xy - 1$ in the polynomial ring $R[x] = \mathbb{Q}[x, y]$, where $R = \mathbb{Q}[y]$. (Note that $R[x]$ has unique factorization!) As an element of $R[x]$, $y + 1 \in R$ is a root since $g(y + 1) = (y + 1)^2 - y(y + 1) - (y + 1) = 0$, but it can be shown by hand that g is irreducible – try it!

Moreover, it is *not* true in general that if a polynomial f of degree at least one has no root, then it is irreducible (even over a field!) For instance, $f(x) = (x^2 + 1)(x^2 + 4) \in \mathbb{Q}[x]$ is irreducible, but has no root in $\mathbb{Q}$! We do know that this is true, however, for polynomials over a field with degree 2 or 3.

Next, we fixed the following **setup** for the rest of our class period: K is an extension field of a field F, and fix $\alpha \in K$.

Then the intersection of all fields in K that contain both F and α is again a field, and it is the minimal subfield of K that contain both F and α. This field is denoted $F(\alpha)$, and we call it a **simple extension** of F, and α a **primitive element** for the extension.

We can apply the same process to obtain a minimal subfield of K containing F and $\alpha_1, \alpha_2, \ldots \in K$, denoted $F(\alpha_1, \alpha_2, \ldots)$, and called the subfield **generated** by $\alpha_1, \alpha_2, \ldots$ over F.

We gave several examples, showing that $\mathbb{C} = \mathbb{R}(i)$, and also equals $\mathbb{R}(-i)$, and noticing that the notation for quadratic fields use the same notation $F(\alpha)$; i.e., $\mathbb{Q}(\sqrt{2})$ is the simple extension of $\mathbb{Q}$ with primitive element $\sqrt{2} \in \mathbb{R}$.

We stated an sketched a proof of the following **theorem**: If $f \in F[x]$ is irreducible, K is an extension field of F, and $\alpha \in K$ is a root of f, then

$$F(\alpha) \cong F[x]/(f).$$

In particular, this shows that given any roots α, β of f in K, $F(\alpha) \cong F(\beta)$; i.e., these simple extensions are "algebraically indistinguishable." As a corollary, we find that if $\deg(f) = n$, then

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\}.$$

Next, we defined what it means for $\alpha \in K$ to be **algebraic** over F: α is a root of some polynomial over F. If α is not algebraic over F, we call it **transcendental** over F. For instance, $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ since i satisfies the equation $x^2 + 1$.

If every element of K is algebraic over F, we say that K is **algebraic** over F.

Note: If $F \subseteq K \subseteq L$ are fields and L is algebraic over F, then it is clear from the definition that K is also algebraic over F.

We then stated a fundamental **theorem**: If $\alpha \in K$ is algebraic over F, then there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ with α as a root. Moreover, any polynomial $f \in F[x]$ with α as a root is a multiple of $m_{\alpha,F}(x)$.

We call $m_{\alpha,F}(x)$ the **minimal polynomial** of α over F, and often denote it $m_\alpha(x)$ if the field F is apparent from the the context. Moreover, we call $\deg m_{\alpha,F}$ the **degree** of α over F.

We proved part of the theorem above, and we'll return to this next time.

Lecture 16: Tuesday, March 26. Throughout class today, F denotes a field. Today we had a very concrete and computational class, where we pursued the following question proposed at the end of class last time:

Question: Given a field F and $f \in F[x]$ with no roots in F, is there a field extension K/F (so that $f \in K[x]$ as well) for which f has a root in K?

We went through some examples, noticing that $K = \mathbb{R}$ works for $f = x^2 - 5 \in \mathbb{Q}[x]$, $\mathbb{C}$ works for $f = x^2 + 5 \in \mathbb{R}[x]$, and $\mathbb{Q}$ itself works for $f = x^2 - 25 \in \mathbb{Q}[x]$. However, we could not immediately determine a field extension K of $\mathbb{F}_2$ for which $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ has a root in K. Note that if p is prime, $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$.

We turned to the question of whether $\mathbb{R}$ is the "smallest" K for which $f = x^2 - 5 \in \mathbb{Q}[x]$ has a root in K. We showed that $\mathbb{Q}$ can be identified as a subfield of the ring

$$K = \mathbb{Q}[x]/(x^2 - 5),$$

which is itself a field because $x^2 - 5$ is irreducible in $\mathbb{Q}[x]$. More specifically, the homomorphism $\mathbb{Q} \to K$ given by $a \mapsto \overline{a}$ is an injective ring homomorphism, so that its image in K is a field isomorphic to $\mathbb{Q}$. Identifying $\mathbb{Q}$ with this subfield, we found that f has root $\overline{x} \in K$, so that K satisfies the conclusion of our proposed question. Finally, we also noticed that K can be identified naturally as a subfield of $\mathbb{R}$, and under this identification, K is *strictly* contained in $\mathbb{R}$.

Next, we went back to our earlier examples, and used an analogous technique to that above to find appropriate field extensions K. One important point is that if the polynomial f is reducible in $F[x]$, it suffices to quotient by one of its *irreducible factor*.

This discussion naturally leads to the statement of the following **theorem**: If $f \in F[x]$ is irreducible, then there exists a field extension K/F containing an *isomorphic copy* of K in which f has a root in K. The **upshot**: By identifying F with its isomorphic copy, this theorem shows that there exists an extension of F in which f has a root.

We gave a detailed sketch of the proof of the theorem; in short, the field K can be taken as $F[x]/(f)$, and we can regard F as a subfield of K by identifying it with its image under the injective homomorphism $F \to K$ given by $a \mapsto \overline{a}$. It is not hard to check that $\overline{x} \in K$ is a root of f under this identification.

With the same notation as the argument above, by studying an example, we notices that the identification of $K = F[x]/(f)$ as a field extension of F makes K a vector space over F. We determined that if θ denotes the element $\overline{x}$ in K (so that, in particular, $\theta \in K$ is a root of f), the elements

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

form a basis for K as a vector space over F. In particular, $[K : F] = n$, and

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + \theta^{n-1} \mid a_0, \ldots, a_{n-1} \in F\}$$

i.e., K consists of all polynomials of degree less than n in the variable θ .

We went through several examples of identifying the extension field $F[x]/(f)$ as a field we are already familiar with (e.g., $\mathbb{R}[x]/(x^2 + 1)$ as $\mathbb{C}$, where $\theta = \overline{x}$ corresponds to i, and $\mathbb{Q}[x]/(x^2 + 1)$ as the quadrative field $\mathbb{Q}(\sqrt{2})$. We also did computations in the field $F[x]/(f)$; i.e., finding the inverse of a nonzero element by using the Euclidean Algorithm and back substitution.

Finally, we mentioned that like the quadratic field $\mathbb{Q}(\sqrt{d})$ sitting between $\mathbb{Q}$ and $\mathbb{R}$ or $\mathbb{C}$, given a field extension K/F, and a polynomial $f \in F$ with root $\alpha \in K$, we can define a field $F(\alpha)$ that sits between F and K. Read about this before next time!

Lecture 15: Thursday, March 21. We started class by recalling that the proof of Gauss' lemma gives the following more specific information: If $f \in \mathbb{Z}[x]$ is reducible and $\deg f \geq 1$, then if $f = gh$ for $g, h \in \mathbb{Q}[x]$, then there exist $a, b \in \mathbb{Q}$ for which $ag, bh \in \mathbb{Z}[x]$, so that f factors in $\mathbb{Z}[x]$ as $(ag)(bh)$.

Next, we recalled how we construct $\mathbb{Q}$ from $\mathbb{Z}$ using an equivalence relation. Motivated by this, we constructed the **field of fractions**, or **quotient field**, Q, of a domain R. We gave several examples.

Given a subset A of a field F, the intersection of all fields contained in F (**subfields** of F) is the smallest field containing A, and is called the field *generated by* A. If R is a domain, then, in fact, the quotient field Q is the smallest field containing R. (We made this statement precise.)

If F is a field, the **prime subfield** of F is the field generated by 1 in F. We showed that the prime subfield of a given field is either $\mathbb{Q}$ (if the characteristic of the field is zero) or $\mathbb{Z}/p\mathbb{Z}$, for p a prime integer (if the characteristic is p).

If $F \subseteq K$ are fields, we say that K is a **extension field** of F, or say that K/F is a **field extension**. Every field is an extension field of its prime subfield.

Given a field extension K/F, multiplication in K makes K a vector space over F, and we call the dimension of K as a vector space over F is denoted $[K : F]$, and called the **index** or **degree** of the extension. We call the extension finite/infinite if its index is finite/infinite, respectively.

Finally, we noted that $\mathbb{C}$ is constructed as a field containing

In fact, we know that $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.

Next time, we will start by addressing the following more general question: Given a field F and $f \in F[x]$ with no roots in F, is there a field extension K/F for which f has a root in K?

Lecture 14: Tuesday, March 19. We started class by recalling the statement of Eisenstein's criterion, and filled in a gap from our proof last time (see below).

Next, we carried out the Euclidean Algorithm for two given polynomials f and g over $\mathbb{Z}/3\mathbb{Z}$ to find their greatest common divisor, and to find a principal generator for the ideal $(f, g) \subseteq \mathbb{Z}/3\mathbb{Z}[x]$.

If F is a field, then $F[x]$ is a domain, and 0 is a prime ideal. On the other hand, if I is a nonzero ideal of $F[x]$, then since $F[x]$ is a principal ideal domain, then $I = (p(x))$, where $p \neq 0$. We showed that I is a prime ideal if and only if p is irreducible in $F[x]$. Then we proved that the maximal ideals of $F[x]$ are exactly the nonzero prime ideals. Every maximal ideal is always prime, and this extra statement says that every nonzero prime ideal is maximal. In other words, given $f \in F[x]$, (f) is a prime ideal in $F[x]$ if and only if f is irreducible.

Next, we defined the **characteristic** of a ring, gave some examples, and then proved that the characteristic of a field is either 0 or a prime integer.

Lecture 13: Thursday, March 7. Today, we started by restating the general **Eisenstein's criterion**: Let P be a prime ideal in a domain R, and let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \in R[x]$, where $n \geq 1$. If $a_0, \ldots, a_{n-1} \in P$, but $a_0 \notin P^2$, then f is irreducible in $R[x]$.

We also stated its corollary in terms of polynomials over $\mathbb{Z}$: If p is a prime integer and $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, where $n \geq 1$. If p divides a_i for all $0 \leq i \leq n-1$, and p^2 does not divide a_0, then f is irreducible in $\mathbb{Z}[x]$ (so also in $\mathbb{Q}[x]$ by Gauss' lemma).

We proved the general statement, but got stuck on one step, which was given as an exercise: Assume that P is a prime ideal of a ring R, and $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$, for which all $a_i \in P$, but $a_0 \notin P^2$. Suppose that $f(x) = a(x)b(x)$ for polynomials $a, b \in R[x]$ of degree less than n. Then we certainly have that $\overline{x^n} = \overline{f(x)} = \overline{a(x)} \cdot \overline{b(x)}$ in $(R/P)[x]$. Our claim is that this means that $\overline{a(x)}$ and $\overline{b(x)}$ both have zero constant term in $(R/P)[x]$ (so that the constant terms of $a(x)$ and $b(x)$ are in P). Try proceeding as follows: Suppose that $\overline{a(x)}$ has a nonzero constant term. Then what is the degree of the lowest degree term of $\overline{a(x)} \cdot \overline{b(x)} = \overline{x^n}$?

We gave several examples of applying Eisenstein's criterion to conclude that a polynomial is irreducible over $\mathbb{Z}$, which sometimes involved using the fact that a polynomial $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. (Notice that the same principle applies more generally!)

From here onward, we considered polynomials in $F[x]$, where F is a field. We defined a **greatest common divisor** of two polynomials described the **Euclidean Algorithm** for polynomials, and stated **Bézout's theorem** for polynomials over a field. We did an example of computing a greatest common divisor, and the unique *monic* greatest common divisor of two polynomials, and then using the steps in the Euclidean Algorithm to find the polynomials guaranteed by Bézout's theorem.

We then used Bézout's theorem to motivate the fact that $F[x]$ is a **principal ideal domain**, meaning that, like the ring $\mathbb{Z}$, it is a domain in which every ideal is principal. We noticed that in polynomial rings over rings that are not fields, not every ideal must be principal (e.g., $(2, x) \subseteq \mathbb{Z}[x]$).

Lecture 12: Thursday, February 28. We began class by reviewing a few simple facts about polynomials f over a field F from last time: First, if f has degree at least one, then it has a linear factor if and only if it has a root; in fact, $a \in F$ is a root if and only if $(x-a) \mid f$. We noted that this implies that a polynomial of degree n over a field has at most n roots. It also implies that If f has degree 2 or 3, then f is irreducible if and only if f has not root in F.

We noticed used this final criterion to check that $f = x^2 + x + 1$ has not root as a polynomials in $\mathbb{Z}/2\mathbb{Z}[x]$, nor as a polynomial in $\mathbb{R}[x]$, but we know it factors in $\mathbb{C}[x]$.

We asked a similar question: Is there is a polynomial that is irreducible in $\mathbb{Q}[x]$ but reducible in $\mathbb{R}[x]$? Yes! For example, $x^2 - 3$.

Similarly, we could ask whether there exists a polynomial that is irreducible in $\mathbb{Z}[x]$ but reducible in $\mathbb{Q}[x]$. Several students had good ideas on ways to approach this, but we were not able to come to any conclusion based on the ideas.

We turned to the study of **rational roots of polynomials with integer coefficients**. First, we stated the following proposition: If

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

and $\frac{r}{s} \in \mathbb{Q}$ is a root of p written in lowest terms, then $r \mid a_0$ and $s \mid a_n$. The proof of this statement is left as a straightforward exercise.

As a consequence of this result, if $p(x)$ is a monic polynomial in $\mathbb{Z}[x]$ such that $p(d) = 0$ for every divisor d of the constant term of p, then p has no rational roots. We used this statement to show that $x^3 - 3x - 1, x^2 - 7$, and $x^3 - 101$ are irreducible in $\mathbb{Q}[x]$.

Next, we stated and proved **Gauss' lemma**, which answers our unresolved question in the negative: Given a polynomial $p(x) \in \mathbb{Z}[x]$, if p is reducible in $\mathbb{Q}[x]$, then p is reducible in $\mathbb{Z}[x]$. Moreover,

We applied Gauss' lemma in several ways, to conclude that certain polynomials over $\mathbb{Z}$ are irreducible over $\mathbb{Q}$: x^4+3x^2+x+5, $(x-1)(x-2)(x-3)(x-4)(x-5)+1$, and $(x-1)(x-2)\cdots(x-100)+1$. In each case, we assumed that the polynomial was reducible over $\mathbb{Q}$, so that by Gauss' lemma, it is reducible over $\mathbb{Z}$; however, we proceeded in different ways in each setting.

Finally, we gave the general statement of **Eisenstein's criterion**: If R is a domain and P is a prime ideal of R, then given

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$$

where $n \geq 1$, if $a_0, a_1, \ldots, a_{n-1} \in P$ and $a_0 \notin P^2$, then f is irreducible in $R[x]$.

Lecture 11: Tuesday, February 26. Throughout class today, R is a commutative ring with 1. We recalled from last time that given an ideal I of R, the ideal of $R[x]$ generated by the set I, (I), is the set of all polynomials with coefficients in I, and we have that

$$R[x]/(I) \cong (R/I)[x]$$

and if I is a prime ideal of R, then (I) is an ideal of $R[x]$. We noted that the final statement is *not* true when "prime" is replaced with "maximal:" In fact, (I, x) is a maximal ideal of $R[x]$ if I is a maximal ideal of R. We also illustrated the isomorphism above for $R = \mathbb{Z}$.

Next, we defined $R[x_1, x_2]$ as the polynomial ring in indeterminate x_2 over the ring $R[x_1]$; i.e., $R[x_1, x_2] = (R[x_1])[x_2]$. Inductively, we can then define a polynomial in a finite set of indeterminates, $R[x_1, \ldots, x_n]$. We gave some examples of elements of the ring $\mathbb{Z}[x, y]$.

Finally, we stated that if F is a field, then the polynomial $F[x]$ satisfies the **Division Algorithm**: Given $a(x), b(x) \in R[x]$, where $b(x)$ is a nonzero polynomial, then there exist unique polynomials $q(x), r(x) \in F[x]$ for which $\deg r(x) < \deg b(x)$, and

$$a(x) = b(x)q(x) + r(x).$$

We gave examples illustrating this, and then examples where the Division Algorithm fails to hold for $R = \mathbb{Z}$ and $R = \mathbb{Z}/6\mathbb{Z}$. We then proved the Division Algorithm for polynomials over fields.

From here, we gave some basic definitions on polynomials. Given polynomials $f, g \in R[x]$, we say that f **divides** g, of write $f \mid g$, if $g = fh$ for some $h \in R[x]$. We say a polynomial is **reducible** if $\deg f \geq 1$ and whenever $f = gh$ for $g, h \in R[x]$, then f or g is a unit. We say that $f, g \in R[x]$ are **associates** if $f = ug$ for u a unit in R.

We gave examples polynomials that are irreducible over certain fields, but reducible over others. We proved that over a field, every linear polynomial is irreducible.

We stated precisely the fact that polynomials $f \in F[x]$ of degree at least one (i.e., f is a nonzero, non-unit of $F[x]$) satisfy **Unique Factorization**: There exist irreducible polynomials $g_1, \ldots, g_n \in F[x]$ for which

$$f(x) = g_1(x) \cdots g_n(x)$$

an if $f(x) = h_1(x) \cdots h_m(x)$ for irreducible polynomials $h_1(x), \ldots, h_m(x) \in F[x]$, then $n = m$ and we can renumber the $h_j(x)$ so that $f_i(x) = h_i(x)$ for all $1 \leq i \leq n$.

From here, we stated and proved the **Root theorem**: Given a polynomial $p(x) \in F[x]$, for F a field, we have that $a \in F$ is a root of $p(x)$ (i.e., $p(a) = 0$) if and only if $(x - a) \mid p$.

Finally, we stated and argued that the following holds: Given a polynomial of degree 2 or 3 over a field, the polynomial is irreducible if and only if it has no root in the field. We finished class by applying this in a few examples.

Lecture 10: Thursday, February 20. Today, we motivated the statement of the *Chinese remainder theorem* in terms of actual remainders, and rings $\mathbb{Z}/n\mathbb{Z}$.

Next, we recalled the definition of what it means for two ideals ot be **comaximal**. We also investivated how to characterize the product of principal ideals.

After this, we stated the general **Chinese remainder theorem** (CRT) in terms of arbitrary ideals, and then the specific case dealing with ideals in the ring of integers. We illustrated the theorem with an example in this case. Next, we proved the general version of the CRT.

After this, we turned to start a more in-depth investigation of polynomial rings. We recalled the facts that if R is a commutative domain with 1, then

- $\deg(pq) = \deg(p) + \deg(q)$ for p, q nonzero elements of $R[x]$.
- The units of $R[x]$ are simply the units of R.
- $R[x]$ is also a domain.

We also showed that given an ideal I of R, the ideal of $R[x]$ generated by the set I, (I), is the set of all polynomials with coefficients in I, and we have that

$$R[x]/(I) \cong (R/I)[x]$$

and if I is a prime ideal of R, then (I) is an ideal of $R[x]$.

Lecture 9: Tuesday, February 19. We started class by recalling that given a commutative ring R with 1, R is a field if and only if its only ideals are 0 and the ring itself. We used this to prove that any nonzero ring homomorphism from a field must be injective (by considering the kernel, an ideal of the field!).

We defined a proper ideal of a ring to be **maximal** if the only ideals containing this ideal are the ideal itself, and the ring. We gave several examples and non-examples of maximal ideals in different rings.

Then we stated a **fact** (whose proof requires *Zorn's lemma*), that in a ring with 1, every proper ideal is contained in some maximal ideal.

We then stated and proved an important theorem: In a commutative ring R, an ideal I is maximal if and only if R/I is a field.

Next, we went back to our earlier examples, and confirmed our conclusions about which ideals are maximal, or made further conclusions in cases where the answer was not immediately clear (e.g., $(2, x)$ in $\mathbb{Z}[x]$). Filling in details is part of the homework (see below!).

After this, we defined what if means for a proper ideal $\mathfrak{p}$ of a commutative ring R to be **prime**: Whenever $a, b \in R$ and $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. This definition is motivated by the notion of a prime integer, and we noticed that the prime ideals of $\mathbb{Z}$ are exactly $p\mathbb{Z}$ for p prime, along with the zero ideal.

In fact, we noticed that 0 is a prime ideal of a commutative ring if and only if the ring is a domain!

We then stated a theorem that says that if R is a commutative ring, an ideal I is prime if and only if R/I is a domain. The proof is assigned as homework (see below)!

We gave examples of prime and non-prime ideals in $\mathbb{Z}[x]$, and saw how $\mathbb{C}$ can be "constructed" from $\mathbb{R}$ using quotient rings (see homework problem #4 below!).

Finally, we noticed that the characterizations of prime and maximal ideals in a commutative ring, in terms of quotients, implies that a *maximal ideal is always prime*.

Finally, we recalled the definition of a **product of rings**, and defined what it means for two ideals in a ring to be **comaximal**.

Additional homework problems

1. Prove that an ideal I of a commutative ring is prime if and only if R/I is a domain.
2. Prove that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.
3. Prove that $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$.

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

Lecture 8: Thursday, February 14. We reviewed the statement of the **first isomorphism theorem** for rints, and noted that it implies that every kernel of a ring homomorphism is an ideal, and vice versa.

Next, we stated and proved the **second isomorphism theorem** for rings. Its proof required the following *essential fact* about ring homomorphisms from quotient rings: Given a ring homomorphism $\varphi : R \to S$, if I is an ideal of R contained in the kernel of φ, then

$$\widetilde{\varphi} : R/I \to S$$

given by $\widetilde{\varphi}(r+I) = \varphi(r)$ is a well-defined ring homomorphism with the same image as the image of φ, and $\widetilde{\varphi}$ is injective if and only if $I = \ker \varphi$. You proved most of this in the quiz earlier today!

Next, we explained carefully the statements of the **third isomorphism theorem** and **fourth**, or **lattice isomorphism theorem** for rings.

From here, we defined a **principal ideal** (a) of a ring R, which is the smallest ideal containing some element $a \in R$, which is called the ideal *generated by* a. Similarly, we defined an ideal *generated by* a collection, or subset, of elements of the ring; if this subset is finite, we call the ideal **finitely generated**.

We noticed that the zero ideal is always principal, and if a ring contains 1, then the ring itself is the principal ideal (1). We argued that every ideal in $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some integer n, so that every ideal of the integers is principal, since $n\mathbb{Z} = (n) = (-n)$.

Next, we turned to studying some ideals in $\mathbb{Z}[x]$. We noticed that the principal ideal (5) can be described as the collection of all polynomials in which every coefficient is a multiple of 5; similarly, (2) is the collection of polynomials with even coefficients.

We recalled our familiar examples of ideals in $\mathbb{Z}[x]$: The ideal of all polynomials with zero constant terms is exactly the principal ideal (x), and the ideal of all polynomials with even constant term is $(2, x)$; we proved that this latter ideal is not principal!

Finally, we proved that given a commutative ring with 1, this ring is a field if and only if its only ideals are the zero ideal, and the ring itself.

Lecture 7: Tuesday, February 12. After recalling the definition of an ideal of a ring, we defined the **sum, product, and powers of a given ideal**, which are all again ideals of the same ring. We noted that the product of two ideals sits in their intersection, another ideal, and that the sum of two ideals is the *smallest* ideal containing both ideals. We gave a precise example in the ring of integers.

Next, we motivated the notion of a *quotient* by studying different spaces, and recalling how we use representative notation freely in, say, fraction notation. We reviewed the Quotient Rings worksheet conclusions, to construct a new ring R/I from a ring R and an ideal I of R.

We went through the three examples on the worksheet, and described the corresponding quotient rings: The ideal $I = n\mathbb{Z}$ of $R = \mathbb{Z}$, the ideal I consisting of all polynomials with zero constant term in $R = \mathbb{Z}[x]$, and J the ideal of this same ring consisting of all polynomials with even constant term. In the last two examples, we saw that the quotient rings can be pretty different from one another with respect to different ideals (e.g., one was finite, and one infinite)! We drew rough "pictures" to represent quotient rings in each case.

Next, we proved that a ring homomorphism is injective if and only if its kernel is the subring consisting only of zero.

After this, we stated a **theorem**: Given an ideal I of a ring R, the function

$$\eta : R \to R/I$$

defined by $\eta(r) = r + I$ is a surjective ring homomorphism with kernel I. This is often called the **natural projection** of R onto R/I. Note that the first step was to show that this function is even well-defined!

We saw this theorem realized in natural ways using our earlier examples. In particular, the natural projection of $\mathbb{Z}$ onto $\mathbb{Z}/n\mathbb{Z}$, and evaluation of a polynomial at a point, are both of the form η above, for appropriate R and I.

From here, we recalled that given a ring homomorphism $\varphi : R \to S$, the kernel of φ is always an ideal of R, and the image is always a subring of S. However, the image need not always be an *ideal* of S: for instance, consider the inclusion $i : \mathbb{Z} \to \mathbb{Q}$.

Finally, we stated the **first isomorphism theorem for rings:** Given a ring homomorphism $\varphi : R \to S$,

- $\ker \varphi$ is an ideal of R,
- $\operatorname{Im} \varphi$ is a subring of S, and
- $R/\ker \varphi \equiv \operatorname{Im} \varphi$.

We proved the remaining (third) statement.

Lecture 6: Thursday, February 7. Today's lecture was canceled due to the closure of the KU campus. The lecture is replaced with the Quotient Rings worksheet, available on the course website. This worksheet leads students to develop the notion of a quotient ring by defining an equivalence relation on a ring R determined by a given ideal I, and checking that the equivalence classes $r + I$, for $r \in R$, form a ring under "inherited" operations of addition and multiplication. This ring is called the **quotient ring** R/I, and the element $r + I$ in this ring is called the **coset** of r in R/I.

Lecture 5: Tuesday, February 5. We started class by returning to the question of what the zero divisors in the ring of *continuous* functions from $[0, 1]$ to $\mathbb{R}$, which Geoffrey figured out consists of all functions that vanish on some nonempty open interval in $[0, 1]$.

We also motivated why we use the convention that the zero polynomial is Then for any two polynomials f, g over any ring, $\deg(fg) \leq \deg(f) + \deg(g)$.

Next, we recalled the definition of a **(ring) homomorphism** and defined the **kernel** of such a function. We also defined a **(ring) isomorphism** as a bijective ring homomorphism.

We investigated ring homomorphisms from $\mathbb{Z}$ to itself, and concluded that the only ones are "trivial:" the zero and identity maps. We also noticed that the only ring homomorphism from $\mathbb{Z}/n/\mathbb{Z}$ to $\mathbb{Z}$ is the zero map. Finally, we gave an example of an *evaluation map* on a polynomial ring,

$$\eta : R[x] \to R$$

where $\eta(p(x)) = p(0)$, which is, in fact, a ring homomorphism.

We stated a **proposition** that given an ring homomorphism $\varphi : R \to S$, the image $\operatorname{Im}\varphi$ is a subring of S, and the kernel $\ker\varphi$ is a subring of R. We proved the latter statement, and noticed that its proof is, in some sense, "too easy." This motivated the following definition.

Next, given a subset I of R, we defined what it means for I to be a **left ideal** of R, and a **right ideal** of R. A subset I that is both a left ideal and a right ideal is simply called an **ideal** of R.

We immediately noticed that if R is commutative, to show that a subset I of R is an ideal, than it is enough to show it is either a right or a left ideal. We also noticed that an I is always subring of R, but if $1 \in I$, then $I = R$. It is also clear that 0 is in any ideal. In fact, it is easy to check that the set containing only the 0 element is an ideal (which we denote as 0), and the entire ring is always an ideal.

We saw that given any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal of the ring of integers $\mathbb{Z}$. We also conjectured that if n, m are elements of the ideal I of $\mathbb{Z}$, then the greatest common divisor (n, m) is also in I (check this!).

We saw that the set of all polynomials with no constant term, along with the zero polynomial, is an ideal in a polynomial ring $R[x]$. On the other hand, the set of polynomials with *even* constant term is an ideal in $\mathbb{Z}[x]$.

Finally, we argued that the only ideals in a field are the 0 ideal, and the entire field.

We stated and proved the fact that $\varphi : R \to S$ is a ring homomorphism, that $\ker\varphi$ is an *ideal* of R. We finished by asking an analogous question: Is $\operatorname{Im}\varphi$ necessarily an ideal of S? As a start, try thinking about homomorphisms $\mathbb{Z} \to \mathbb{R}$!

Lecture 4: Thursday, January 31. Today, we had a second guest lecture by Professor Hailong Dao. Class began by finishing the discussion on the **degree** of a polynomial over a commutative ring R; i.e., an element the polynomial ring $R[x]$. We finished proving that when R is a domain and f and g are nonzero polynomials in $R[x]$, then

$$\deg(fg) = \deg(f) + \deg(g).$$

Moreover, we noticed that the degree of a constant in R is zero, and our convention is that the degree of the zero polynomial is $-\infty$. Using these, facts we proved that when R is a domain, then $R[x]$ is also domain, and the units of $[x]$ are exactly the units of R.

Next, given a ring R, we defined and discussed the **ring of $n \times n$ matrices**, $M_n(R)$, over R. We explained why the set of upper triangular matrices is a subring of $M_n(R)$.

Finally, we defined a **ring homomorphism** and a **ring isomorphism**. We investigated several examples: the identity map on a ring, the zero map on a ring, and homomorphisms between the integers $\mathbb{Z}$ and the ring $\mathbb{Z}/n\mathbb{Z}$.

Lecture 3: Tuesday, January 29. Today, we had a guest lecture from Professor Hailong Dao. First, we proved that any finite domain must be a field.

Next, we defined a **subring** of a ring (without referencing the definition of a "group"). Next, we argued that to verify that a subset of a ring that is a subring, we must only check it is nonempty and closed under subtraction and multiplication.

After this, we explained how to verify that $S = \mathbb{Q}[\sqrt{2}]$ is a subring of the ring of real numbers $\mathbb{R}$. We also saw that S is a field, and$\mathbb{Z}[\sqrt{2}]$ is a subring of S. We also mentioned how extensions of $\mathbb{Q}$ or $\mathbb{Z}$ arise from trying to understand equations like $x^2 - 2y^2 = 1$ or $x^3 + y^3 = z^3$.

Finally, we defined a **polynomial** over a given commutative ring R. The polynomials form a ring, called a **polynomial ring**, which is denoted $R[x]$. We stated that when R is a domain, and g and h are nonzero polynomials, then $\deg(gh) = \deg(g) + \deg(h)$.

Lecture 2: Thursday, January 24. We started class by reviewing the definition of a ring, a commutative ring, and a ring with unity/identity. We also reviewed what it means for an element of a ring to be a zero divisor, or a unit. We showed that an element cannot simultaneously be a zero divisor and a unit.

Next, we described all units and zero divisors of the ring of functions from the closed unit interval to $\mathbb{R}$, and saw that every nonzero function is one or the other. On the other hand, we demonstrated that in the ring of continuous functions on the same set that a function be neither a unit nor a zero divisor.

We defined an **integral domain**, often just called a **domain**, as a commutative ring with identity that contains no zero divisors.

We then proved that whenever a, b, c are elements of a ring, and a is a nonzero element that is not a zero divisor, we can cancel by a, meaning that if $ab = ac$, then $b = c$. In particular, this implies that we can *always* cancel by nonzero elements in a domain.

We defined a **field** as a commutative ring with $1 \neq 0$ in which all nonzero elements are units.

We noticed that every field is a domain, and $\mathbb{Z}$ is a domain that is not a field, while $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields (so also domains). We drew a chart comparing these types of rings, and filled in all our examples of rings thus far. Missing was an important example of the integers modulo n, so we began our construction of this ring.

Toward this goal, we defined an **equivalence relation on a set**, and corresponding **equivalence classes**, and gave several examples. We noticed that the equivalence classes partition the set.

Although we will use other important examples soon, our most important example today was the following equivalence relation on the set of integers $\mathbb{Z}$: given an integer $n \geq 2$, a b if and only if $a \equiv b \bmod n$ (i.e., $n \mid (b-a)$). We studied the equivalence classes in this case, which are often called **congruence classes**; the equivalence class of $a \in \mathbb{Z}$ is denoted $\overline{a}$ (although the bar is sometimes suppressed for clarity of notation). The set of congruence classes form a ring, and addition and multiplication are defined as:

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Of course, it is not immediately that these are well-defined operations, and form a ring; you are required to check this on your own if you are familiar with the arguments. We define $\mathbb{Z}/n\mathbb{Z}$ as this ring of congruence classes; i.e.,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

The ring $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with unity, and we proved that its zero divisors are the elements $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ such that a and n are relatively prime. On the other hand, we showed that the zero divisors are precisely all nonzero elements that are not units; i.e., all $\overline{a}$ such that a has a common divisor with n.

Using this, we deduced that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime. We used this to put this ring in our chart in two cases: n prime, and n composite.

Lecture 1: Tuesday, January 22. Today, we started class by going over the course syllabus, course requirements, and course website.

Next, we defined a **ring**, which consists of a set and two binary operations, which we call addition and multiplication, and denote "+" and "·", satisfying several axioms:

- *Addition* satisfies:
  - *associativity*,
  - existence of an **additive identity** ("**zero**/0"),
  - existence of **multiplicative inverses** ("**negatives**"), and
  - *commutativity*.
- *Multiplication* satisfies *associativity*.
- The *Distributive Law* holds.

The first four axioms involving addition say that a ring is an **abelian group** under addition, and the property of distributivity essentially says that the two operations are compatible with one another.

We gave several examples of rings, starting with the set motivating the definition, the set $\mathbb{Z}$ of integers, using the typical operations of addition and multiplication. The larger sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are also rings. The **trivial ring** consisting only of the zero element is not ideal, since often we want to use a ring with a **multiplicative identity** ("1", often just called an **identity**, or **unity**) that is distinct from 0. We defined what it means for a ring to have a multiplicative identity. The ring $2\mathbb{Z}$ consisting of all even integers has no identity.

We defined what it means for a ring to be commutative, and gave the example of the ring $M_n(\mathbb{R})$ of all $n \times n$ matrices with real entries as a non-commutative ring. We noticed that $\mathbb{R}$ can be replaced with $\mathbb{Q}$ or $\mathbb{C}$, or even an arbitrary ring itself, and we obtain other rings of matrices. We then defined various rings of functions.

Next, we proved that the additive inverse of a ring element is unique. A similar argument shows that the additive identity is also unique.

We then stated a proposition: Given a ring R, for all $a, b \in R$, the following hold.

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a)b = a(-b) = -ab$
3. $(-a)(-b) = -ab$
4. If R has a multiplicative identity, then it is unique, and $-a = (-1)a$

We proved one equality in each of (1) and (2), and the remainder are assigned as homework.

Next, we defined what it means for an element to be a **zero divisor** or a **unit** of a ring. The set of all units in a ring R is denoted $R^\times$. We saw that the ring of integers $\mathbb{Z}$ has no zero divisors, and its only units are ± 1.

We turned to rings of functions, starting with all functions from $[0, 1]$ to $\mathbb{R}$. Think about what functions are zero divisors in this ring, and which are units.