SPRING 2024: MATH 791 DAILY UPDATE

Monday, April 29. The class worked in teams on Exam 3.

Friday, April 26. The class worked in teams on Exam 3.

Wednesday, April 24. We spent most of the class following the proof of the Inverse Galois Problem for cyclic groups to construct a field K such that K is a Galois extension of $\mathbb{Q}$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_8$. For this, the first prime p such that $p \equiv 1 \bmod 8$ is 17. Thus, if ϵ is a primitive 17th root of unity, $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q}) \cong \mathbb{Z}_{17}^*$, which is a cyclic group of order 16. To find a Galois extension K of $\mathbb{Q}$ whose Galois group is isomorphic to $\mathbb{Z}_8$, we must take the fixed field of H, where $H \subseteq \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ is a subgroup of index 8. Now, $\overline{5}$ is a cyclic generator for $\mathbb{Z}_{17}^*$ (check this), and it followed that $\sigma \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ given by $\sigma(\epsilon) = \epsilon^5$ is a cyclic generator of $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. Therefore σ^8 is an element of order two, and so it generates a subgroup of index 8. If we call this subgroup H, then $\gamma \in \mathbb{Q}(\epsilon)$ is in the fixed field of H if and only if $\sigma^8(\gamma) = \gamma$

Now, the minimal polynomial for ϵ over $\mathbb{Q}$ is $\Phi_{17}(x) = x^{16} + x^{15} + \cdots + x + 1$, so that $1, \epsilon, \ldots, \epsilon^{15}$ is a basis for $\mathbb{Q}(\epsilon)$ over $\mathbb{Q}$. Thus, if $\gamma \in \mathbb{Q}(\epsilon)$, we can write

$$\gamma = a_0 + a_1\epsilon + a_2\epsilon^2 + \cdots + a_{15}\epsilon^{15},$$

and therefore,

$$\sigma^8(\gamma) = a_0 + a_1\sigma^8(\epsilon) + a_2\sigma^8(\epsilon^2) + \cdots + a_{15}\sigma^8(\epsilon^{15}).$$

A somewhat tedious (though not difficult) calculation shows that

$$\begin{aligned}
\sigma^8(\epsilon) &= -1 - \epsilon - \epsilon^2 - \cdots - \epsilon^{15}\\
\sigma^8(\epsilon^2) &= \epsilon^{15}, \sigma^8(\epsilon^3) = e^{14}, \sigma^8(\epsilon^4) = \epsilon^{13}\\
\sigma^8(\epsilon^5) &= \epsilon^{12}, \sigma^8(\epsilon^6) = \epsilon^{11}, \sigma^8(e^7) = \epsilon^{10}\\
\sigma^8(\epsilon^8) &= \epsilon^9, \sigma^8(\epsilon^9) = \epsilon^8, \sigma^8(\epsilon^{10}) = \epsilon^7\\
\sigma^8(\epsilon^{11}) &= \epsilon^6, \sigma^8(\epsilon^{12}) = \epsilon^5, \sigma^8(\epsilon^{13}) = \epsilon^4\\
\sigma^8(\epsilon^{13}) &= \epsilon^4, \sigma^8(\epsilon^{14}) = \epsilon^3, \sigma^8(\epsilon^{15}) = \epsilon^2.
\end{aligned}$$

It follows that

$$\sigma^8(\gamma) = (a_0 - a_1) + (-a_1)\epsilon + (a_{15} - a_1)\epsilon^2 + (a_{14} - a_1)\epsilon^3 + \cdots + (a_2 - a_1)\epsilon^{15}.$$

Setting $\gamma = \sigma^8(\gamma)$, we obtain

$$a_0 = a_0, a_1 = 0, a_2 = a_{15}, a_3 = a_{14}, a_3 = a_{13}, \ldots, a_{14} = a_3, a_{15} = a_2.$$

Therefore,

$$\gamma = a_0 + a_2(\epsilon^2 + \epsilon^{15}) + a_3(\epsilon^3 + \epsilon^{14}) + \cdots + a_6(\epsilon^6 + \epsilon^{11}) + a_7(\epsilon^7 + \epsilon^{10}) + a_8(\epsilon^8 + \epsilon^9).$$

It follows that $K := \mathbb{Q}(\epsilon^2+\epsilon^{15}, \epsilon^3+\epsilon^{14}, \ldots, \epsilon^6+\epsilon^{11}, \epsilon^7+\epsilon^{10}, \epsilon^8+\epsilon^9)$ is the fixed field of H, and $\mathrm{gal}(K/\mathbb{Q}) \cong \mathbb{Z}_8$, as required. We can simplify K by noting that

$$\begin{aligned}
(\epsilon^2 + \epsilon^{15})^2 &= \epsilon^4 + 2 + \epsilon^{13}\\
(\epsilon^3 + \epsilon^{14})^2 &= \epsilon^6 + 2 + \epsilon^{11}\\
(\epsilon^5 + \epsilon^{12})^2 &= \epsilon^{10} + 2 + \epsilon^7\\
(\epsilon^4 + \epsilon^{13})^2 &= \epsilon^8 + 2 + \epsilon^9
\end{aligned}$$

It follows that $K = \mathbb{Q}(\epsilon^2 + \epsilon^{15}, \epsilon^3 + \epsilon^{14}, \epsilon^5 + \epsilon^{12})$. Can you find a simpler expression for K? $\square$

We ended class by sketching a proof of the following theorem:

Theorem. Let G be a finite group. Then there exists a finite, Galois extension of fields $F \subseteq K$ such that $\mathrm{Gal}(K/F) \cong G$.

If $|G| = n$, the idea of the proof was to let K be the rational function field in n variables over $\mathbb{Q}$ and to let S_n be the group of automorphisms of K obtained by permuting the given variables. Letting F_0 denote the field of symmetric rational functions, i.e., the fixed file K^{S_n}, then by a theorem of E. Artin, $\mathrm{Gal}(K/F_0) = S_n$ and K is Galois over F_0. Identifying G as a subgroup of S_n and taking F to be the fixed field K^G, it follows from the Galois Correspondence Theorem that $F \subseteq K$ is a Galois extension with Galois group G.

Monday, April 22. After reviewing the the statement of the Galois Correspondence Theorem, we illustrated the theorem by calculating the intermediate fields and corresponding subgroups of the Galois groups for the two extensions: $\mathbb{Q} \subseteq \sqrt{2}, \sqrt{3})$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \epsilon)$, where $\epsilon = e^{\frac{2\pi i}{3}}$. This was made easy by the fact that we had previously calculated both Galois groups and the fixed fields of the first extension. The second example had the advantage of having intermediate fields not Galois over $\mathbb{Q}$ that correspond to subgroups of the Galois group that are not normal subgroups.

We then mentioned the well-known (and not fully determined!):

Inverse Galois Problem. Is every finite group the Galois group of a Galois extension of $\mathbb{Q}$?

We ended class by showing that the Inverse Galois Problem has a positive solution for $G = \mathbb{Z}_n$, assuming the following special case of Dirichlet's Theorem: For n fixed, there exist (infinitely many) prime numbers in the arithmetic progression $\{mn + 1\}_{m \geq 1}$. Another key ingredient of the proof was that for p prime, the multiplicative group $(\mathbb{Z}_p)^*$ is cyclic, a fact we recorded when we showed that a finite extension of finite fields always has a primitive element.

Friday, April 19. We continued our discussion of Galois groups and Galois extensions by first offering the following theorem.

Theorem. Suppose that $F \subseteq K$ is a finite extension with a primitive element, so that $K = F(\alpha)$. Let $p(x)$ denote the minimal polynomial of α over F and write $d = \deg(p(x))$. Then K is Galois over F if and only if $p(x)$ has d-distinct roots in K. Moreover, if $\mathbb{Q} \subseteq F$, then the following are equivalent: (a) K is Galois over F; (b) K is the splitting field of $p(x)$ over F; (c) K is the splitting field of some $f(x) \in F[x]$ over F.

We noted that the first part of theorem follows immediately from the Crucial Proposition from the lecture of April 12, while the second equivalences follow from the first statement and the proposition on splitting fields proven in the previous lecture.

We then established the following facts: (i) Any finite extension of finite fields is a Galois extension and (ii) If $F = \mathbb{Z}_2(t^2)$, $K = \mathbb{Z}_2(t)$, $\alpha := t$, then $K = F(\alpha)$ is the splitting field of $p(x) = x^2 - t^2$ over F, yet the extension is not a Galois extension.

We then defined the concept fixed field. Let $F \subseteq K$ be a finite extension with Galois group $\mathrm{Gal}(K/F)$. For $\sigma \in \mathrm{Gal}(K/F)$, $K^\sigma := \{\alpha \in K \mid \sigma(\alpha) = \alpha\}$ if the *fixed field* of σ. For H a subgroup of $\mathrm{Gal}(K/F)$, $K^H := \{\alpha \in K \mid \sigma(\alpha) = \alpha, \text{ for all } \sigma \in H\}$ is the *fixed field* of H. We showed that the fixed fields are intermediate fields between F and K and also calculated the fixed fields of the subgroups of $\mathrm{Gal}(K/F)$ when $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We ended class by mentioning the correspondence between intermediate fields between F and K, when K is Galois over F, and subgroups of the Galois group.

Wednesday, April 17. We spent most of the class proving the crucial proposition from the lecture of April 12, giving a hands-on proof exploiting the division algorithm in the isomorphic rings $F_1[x]$ and $F_2[x]$. We finished class by proving the following theorem, which can be viewed as a corollary to the Crucial Proposition. The theorem plays a key role in identifying Galois extensions $F \subseteq K$ as splitting fields, when either $\mathbb{Q} \subseteq F$ or $|F| < \infty$.

Theorem. Let $F \subseteq K$ be fields such that K is the splitting field of $f(x) \in F[x]$ over F. If the irreducible polynomial $p(x) \in F[x]$ as a root in K, then it splits over K.

Monday, April 15. We began class by restating the crucial proposition presented in the previous lecture and using it to finish the calculation showing that the Galois group of $K := \mathbb{Q}(\sqrt[3]{2}, \epsilon)$ over $\mathbb{Q}$ is isomorphic to S_3

by explicitly exhibiting all of the automorphisms of K over $\mathbb{Q}$. We then recorded the following consequences of the crucial proposition:

(i) If $p(x) \in F[x]$ is irreducible over F and $\alpha_1, \alpha_2 \in \overline{F}$ are two roots of $p(x)$, then there is an isomorphism from $F(\alpha_1)$ to $F(\alpha_2)$ fixing F and taking α_1 to α_2.

(ii) If $K = F(\alpha)$, for α algebraic over F (e.g., $\mathbb{Q} \subseteq F$ or $|F| < \infty$), then $|\mathrm{Gal}(K/F)|$ equals the number of distinct roots of $p(x)$ in K, where $p(x)$ is the minimal polynomial of α over F.

We also noted, but did not prove, that $|\mathrm{Gal}(K/F)| \leq [K : F]$, for any finite extension $F \subseteq K$, and defined in general, the extension to be a *Galois extension* if $[K : F] = |\mathrm{Gal}(K/F)|$. We then gave three examples of Galois extensions and one example of an extension that is not Galois. This lead to the following statement, whose proof is reserved for the next lecture.

Theorem. Let $F \subseteq K$ be a finite extension of fields, such that $\mathbb{Q} \subseteq F$ or $|F| < \infty$. Then K is Galois over F if and only if K is the splitting field over F of a polynomial with coefficients in F.

Friday, April 12. After reviewing the definition of $\mathrm{Gal}(K/F)$ for the field extension $F \subseteq K$, we stated and discussed (but did not prove) the following proposition as a means to construct elements of $\mathrm{Gal}(K/F)$.

Crucial Proposition. Let $F_1 \subseteq K_1$, $F_2 \subseteq K_2$ be fields, $p_1(x) \in F_1]$, $p_2(x) \in F_2[x]$ be monic irreducible polynomials of degree d, and $\alpha_1 \in K_1, \alpha_2 \in K_2$ roots of $p_1(x)$ and $p_2(x)$, respectively. Suppose $\sigma : F_1 \to F_2$ is an isomorphism such that $p_2(x) = p_1(x)^\sigma$. Then there exists an isomorphism $\tilde{\sigma} : F_1(\alpha_1) \to F_2(\alpha_2)$ extending σ such that $\tilde{\sigma}(\alpha_1) = \alpha_2$.

We noted that in the proposition, $p_1(x)^\sigma$ denotes the polynomial in $F_2[x]$ obtained by applying σ to the coefficients of $p_1(x)$.

We then noted the following special cases:

1. If $F = F_1 = F_2$, $K = K_1 = K_2$, $\alpha_1, \alpha_2 \in K$ have minimal polynomial $p(x) \in F[x]$, and $\sigma : F \to F$ the identity map, then there exists an isomorphism of fields $\tilde{\sigma} : F(\alpha_1) \to F(\alpha_2)$ such that $\tilde{\sigma}(\alpha_1) = \alpha_2$.

2. For $F_1 = \mathbb{Q}(\sqrt[3]{2})$ and $F_2 = \mathbb{Q}(\sqrt[3]{2}\epsilon)$, by the special case in 1, we have a field isomorphism $\sigma : F_1 \to F_2$ taking $\sqrt[3]{2}$ to $\sqrt[3]{2}\epsilon$.

$$K_1 = K = K_2 = F_1(\epsilon) = F_2(\epsilon) = \mathbb{Q}(\sqrt[3]{2}, \epsilon),$$

we can extend σ to $\tilde{\sigma} : K \to K$, an automorphism taking ϵ to ϵ^2. This followed from the proposition because $x^2 + x + 1$ is the minimal polynomial both for ϵ over F_1 and ϵ^2 over F_2. We noted that since K is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, if we label its roots as $r_1 = \sqrt[3]{2}, r_2 = \sqrt[3]{2}\epsilon, r_3 = \sqrt[3]{2}\epsilon^2$, then $\tilde{\sigma}$ corresponds to the permutation $(1, 2)$ in S_3. Similarly, we can extend σ to an automorphism $\hat{\sigma}$ of K that takes ϵ to ϵ, noting that $\hat{\sigma}$ corresponds to the permutation $(1, 2, 3)$.

We ended class by first recalling the homework problem that if $\sigma \in \mathrm{Gal}(K/F)$, and $\alpha \in K$ has minimal polynomial $p(x)$, then $\sigma(\alpha)$ is also a root of $p(x)$, and noting that the following corollary is an immediate consequence of the proposition.

Corollary-Definition. Suppose $K = F(\alpha)$ is a finite simple extension and $p(x)$ is the minimal polynomial of α over F. Then $|\mathrm{Gal}(K/F)|$ equals the number of roots of $p(x)$ in K, which is less than or equal to $[K : F]$. If $[K : F] = |\mathrm{Gal}(K/F)|$, we say that K is a *Galois extension* of F.

Wednesday, April 10. Most of the class was devoted to proving the following theorem.

Theorem. Let F be a field, then there exists an algebraic closure for F, i.e., a field $F \subseteq \overline{F}$ such that $\overline{F}$ is algebraically closed and algebraic over F.

We gave the well known proof due to E. Artin, that begins by constructing a field $F \subseteq F_1$ such that every non-zero, non-constant polynomial in $F[x]$ has a root in F_1. For this one takes $F_1 := R/M$, where R is the polynomial ring in the set of variables $\{x_f\}$, one variable for each non-zero, non-constant $f \in F[x]$ and M any maximal ideal containing all $f(x_f)$. That such an M exists follows from earlier results in class. One then iterates this construction and uses various proerties of algebraic extension to get the result.

We finished class by defining $\mathrm{Gal}(K/F)$, the Galois group of K over F, for any field extension $F \subseteq K$, as the group of automorphisms of K fixing F.

Monday, April 8. We began class with the following proposition and its corollary, which are relevant to a study of Galois theory.

Proposition. Let $F \subseteq K$ be a finite extension, with F an infinite field. Then there is a primitive element for the extension if and only if there are (only) finitely many intermediate fields $F \subseteq E \subseteq K$.

A key observation in the proof of the proposition was that if $K = F(\alpha)$ is a simple extension, then the intermediate fields E between F and K correspond to factors of the minimal polynomial $f(x)$ of α over F, as an element of $K[x]$.

Corollary. Let $F \subseteq K$ be a finite extension of fields, with $\mathbb{Q} \subseteq F$. Then there are only finitely many intermediate fields $F \subseteq E \subseteq K$.

We then reviewed the following facts for a field extension $F \subseteq K$:

(i) If $\alpha, \beta \in K$ are algebraic over F, then $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$ are algebraic over F.
(ii) The set E of elements in K that are algebraic over F form a subfield of K containing F, called the *algebraic closure of F in K*.

This was followed by a discussion and proof of the following theorem:

Theorem let $F \subseteq K \subseteq K$ be fields. If E is algebraic over F and K is algebraic over E, then K is algebraic ver F.

We then noted that if E is the algebraic closure of F in K, then E is *algebraically closed* in K, i.e., E equals the algebraic closure of E in K. T

We ended class by defining the concept of an *algebraically closed* field, and what is problematic about constructing and extension $F \subseteq \overline{F}$, where F is both algebraically closed and and algebraic extension of F.

Friday, April 5. We began class by giving the following definition. We began class by proving the following:

Observation. If $F \subseteq K$ is a finite extension of fields, then α is algebraic over F, fr all $\alpha \in K$. The proof followed by using the same determinant trick from the previous lecture. We then proceeded to discuss and prove the:

We then stated and proved the following version of the primitive element theorem.

Theorem. Suppose $F \subseteq K$ is an extension of fields satisfying $[K : F] < \infty$. If $\mathbb{Q} \subseteq F$ or F is finite, then there exists a primitive element $\alpha \in K$ such that $K = F(\alpha)$.

When $\mathbb{Q} \subseteq F$, the proof quickly reduced to the case that $K = F(u, v)$ and ultimately showed that, in this case, for all but finitely many $\lambda \in F$, $\alpha := u + \lambda v$ is a primitive element. When F is finite, we appealed to the standard fact that a finite abelian group is a direct product of cyclic groups. This lead to the fact that the multiplicative group $(K\backslash\{0\}, \cdot)$ is cyclic, and if $\alpha \in K$ is a cyclic generator, then $K = F(\alpha)$.

We then showed that if $F := \mathbb{Z}_2(x^2, y^2)$ is the rational function field in x^2, y^2 over $\mathbb{Z}_2$ and $K = \mathbb{Z}_2(x, y)$, then K is a finite extension of F (of degree four) and there is no primitive element for this extension.

This was followed by establishing the following important proposition, which follows immediately from the observation above and the lecture of March 27.

Proposition. For $F \subseteq K$ fields and $\alpha \in K$, α is algebraic over K if and only if $[F(\alpha) : F] < \infty$.

We ended class by showing that if $F \subseteq K$are fields and $\alpha, \beta \in K$ are algebraic over F, $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$ are algebraic over F.

Wednesday, April 3. We began class by showing that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. The key point here was that $p(x) = x^4 - 10x^2 + 1$ is irreducible and has $\sqrt{2} + \sqrt{3}$ as a root. We arrived at $p(x)$ by starting with the basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, multiplying each basis element by $\sqrt{2} + \sqrt{3}$, and writing the result in terms of the basis with coefficients in $\mathbb{Q}$. This gave rise to a 4×4 homogeneous system of equations with non-trivial solution. The determinant of the coefficient matrix for this system was $p(\sqrt{2} + \sqrt{3})$, which is therefore zero.

We then defined the concept of *primitive element*: For a finite extension of fields $F \subseteq K$, $\alpha \in K$ is a primitive element, if $K = F(\alpha)$. The purpose of the example above was to motivate the following version of the *Primitive Element Theorem.*

Theorem. Suppose $F \subseteq K$ is an extension of fields satisfying $[K : F] < \infty$. If $\mathbb{Q} \subseteq F$, then there exists a primitive element $\alpha \in K$ such that $K = F(\alpha)$.

As a tool for proving the Primitive Element Theorem, we proved the following proposition:

Proposition. Let $0 \neq f(x) \in F[x]$ be a non-constant polynomial. The following are equivalent:

(i) $\text{GCD}(f(x), f'(x)) = 1$
(ii) $f(x)$ and $f'(x)$ have no root in common (say, in the splitting field of $f(x)f'(x)$ over F).
(iii) $f(x)$ has distinct roots in its splitting field over F.

This immediately gave rise to the following corollary, which plays a key role in the proof of the primitive element theorem.

Corollary. If F is a field containing $\mathbb{Q}$ and $p(x) \in F[x]$ is irreducible, then $p(x)$ has distinct roots in K, the splitting of $p(x)$ over F.

This was followed by noting that the corollary above fails, if F does not contain $\mathbb{Q}$. Taking $F := \mathbb{Z}_2(t^2)$ and $K := \mathbb{Z}_t(t)$, the rational function fields over $\mathbb{Z}_2$ in the variables t^2 and t. Then $p(x) = x^2 - t^2$ is irreducible over F, but has the repeated root t in its splitting field K, since $p(x) = (x - t)^2$ over K. Thus, $p(x)$ is an irreducible polynomial with a repeated root in its splitting field.

Monday, April 1. We began by observing that the splitting fields for $x^2 - 2$ and $x^2 + 1$ over $\mathbb{Q}$ are $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$, respectively, and that $[\mathbb{Q}(\sqrt{2} : \mathbb{Q}] = 2 = [\mathbb{Q}(i) : \mathbb{Q}]$. We then noted that the splitting field for $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\epsilon, \sqrt[3]{2}\epsilon^2) = \mathbb{Q}(\sqrt[3]{2}, \epsilon)$, where $\epsilon := e^{\frac{2\pi i}{3}}$ is a primitive cube root of 1. Since ϵ and ϵ^2 are roots of $x^2 + x + 1$, we saw that $\epsilon, \epsilon^2(\text{in order}) = \frac{-1 \pm \sqrt{3}i}{2}$. To calculate $[\mathbb{Q}(\sqrt[3]{2}, \epsilon) : \mathbb{Q}]$, we needed the following proposition, which yields: $[\mathbb{Q}(\sqrt[3]{2}, \epsilon) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \epsilon) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$.

We also gave a **very informal** discussion of Louiville's Theorem from complex analysis and how it is used to prove that every polynomial with complex coefficients has a root in $\mathbb{C}$, and this $\mathbb{C}$ every polynomial with complex coefficients factors as a product of linear polynomials over $\mathbb{C}$. This was followed by a proof of the following:

Proposition. *Let $F \subseteq K \subseteq L$ be fields. Then $[L : F]$ is finite if and only if $[L : K]$ and $[K : F]$ are finite, in which case, $[L : F] = [L : K] \cdot [K : F]$.*

The proof of the proposition followed by showing that if $w_1, \ldots, w_t \in L$ form a basis for L over K and $v_1, \ldots, v_r \in K$ form a basis for K over F, then $\{v_i w_j\}_{1 \leq i \leq r, 1 \leq j \leq t}$ forms a basis for L over F.

Friday, March 29. We gave a hands on proof of the following theorem: Let F be a field, $p(x) \in F[x]$ a non-constant polynomial. Then there exists a field K containing F and $\alpha \in K$ such that $p(\alpha) = 0$. By hands on, we mean we did not just write $K := F[x]/\langle p(x) \rangle$ in the case $p(x)$ is irreducible and argue that K is a field and $\alpha := \overline{x}$ is a root of $p(x)$, which is the standard proof. Though we did note this at the end of class by observing $p(\overline{x}) = \overline{p(x)} = \overline{0}$ in $F[x]/\langle p(x) \rangle$. Instead, we took a new variable which we called z and considered the set $K := \{a_0 + a_1 z + \cdots + a_{d-1} z^{d-1} \mid a_j \in F\} \subseteq F[z]$, and defined addition and multiplication on K as follows: For $A = a_0 + a_1 z + \cdots + a_{d-1} z^{d-1}$ and $B = b_0 + b_1 z + \cdots + b_{d-1} z^{d-1}$,

$$A + B := (a_0 + b_0) + (a_1 + b_1)\alpha + \cdots + (a_{d-1} + b_{d-1})\alpha^{d-1} \quad \text{and} \quad A * B := r(z),$$

where $A(x)B(x) = p(x)q(x) + r(x)$, according to the division algorithm, and $A(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1}$ and $B(x) = b_0 + b_1 x + \cdots + b_{d-1} x^{d-1}$. We then showed that, with these operations, K is a field containing F and $p(z) = 0$. The point of this construction is to observe that, when we already have K and α, a root of $p(x)$, as in the previous lecture, addition and multiplication in $F(\alpha)$ tells us what we should expect when we do not, *a priori*, have α and K. Of course this construction just makes apparent what is really going on in the standard abstract proof noted above.

We finished class by observing that if $f(x) \in F[x]$ is any non-zero, non-constant polynomial, then the theorem can first be extended to finding $F \subseteq K$ and $\alpha \in K$ with $f(\alpha) = 0$, and that this last result can be iterated to show that, for any non-zero, non-constant $f(x) \in F[x]$ having degree d, there exists a field E containing F and $\alpha_1, \ldots, \alpha_d \in E$, not necessarily distinct, such that $f(x) = (x - \alpha_1) \cdots (x - \alpha_d)$. We say that $f(x)$ *splits* over E. The field $F(\alpha_1, \ldots, \alpha_d)$ is called a *splitting field for $f(x)$ over F*.

Wednesday, March 27. We continued our discussion of fields by noting that we want to generalize the constructions from the previous lecture, where we began with the field $\mathbb{Q}$, particular irreducible polynomials over $\mathbb{Q}$ with a designated root, and used this information to construct new fields. We therefore, want to start with fields $F \subseteq K$, $\alpha \in K$ a root of an irreducible polynomial over F and construct a new field $F(\alpha)$. We first began by proving properties of the monic polynomial $p(x) \in F[x]$ of least degree with $p(\alpha) = 0$. We noted that $p(x)$ has the properties: (i) $p(x)$ is irreducible over F; (ii) $p(x)$ divides any $g(x) \in F[x]$ having α as a root and (iii) $p(x)$ is unique. We noted $p(x)$ is called the *minimal polynomial of α over F*. We then showed that if $F \subseteq K$ are fields, and $\alpha \in K$ has minimal polynomial $p(x)$ with degree $d > 0$, then

$F(\alpha) := \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}\}$ is a field, and that $F(\alpha)$ is the smallest subfield of K containing F and α.

This was followed by giving the following important definition.

Definition. Let $F \subseteq K$ be field, and $\alpha \in K$. Then α is *algebraic over F* if α is a root of a polynomial with coefficients in F. It follows then that α also has a minimal polynomial over F.

We then noted that there are just countably many real numbers that are algebraic over $\mathbb{Q}$. This means that there are uncountably many real numbers that are *not* algebraic over $\mathbb{Q}$. Such numbers are called *transcendental numbers.* We noted that it is well known, but difficult to prove, that e and π are transcendental numbers.

We also noted that the minimal polynomial of α over F depends on F: If we set $F := \mathbb{Q}(\sqrt{2})$, $\alpha := \sqrt[4]{2}$, and $K := \mathbb{R}$, then the minimal polynomial of α over $\mathbb{Q}$ is $x^4 - 2$, while the minimal polynomial of α over F is $x^2 - \sqrt{2}$.

Monday, March 25. We began by defining a field F to be a commutative ring in which every non-zero element has a multiplicative inverse. We noted the following familiar examples of fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_p$, p a prime. We also noted rings like $\mathbb{Z}$ and $\mathbb{Q}[x]$ are not fields. We then constructed several other examples of fields, including the following:

(i) $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, a subfield of $\mathbb{R}$.
(ii) $\mathbb{Q}(i) := \{a + bi \mid a, b \in \mathbb{Q}\}$, a subfield of $\mathbb{C}$.
(iii) $\mathbb{Q}(\sqrt[3]{2}) := \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, a subfield of $\mathbb{R}$.

For (iii), we noted that $E := \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ is *not* a field, since $\sqrt[3]{2} \cdot \sqrt[3]{2}$ does not belong to E. The proof of this required the observation that $x^3 - 2$ is irreducible over $\mathbb{Q}$. Using Bezout's Principle in $\mathbb{Q}[x]$, we were able to show that non-zero elements in $\mathbb{Q}(\sqrt[3]{2})$ as defined in (iii) have multiplicative inverses in $\mathbb{Q}(\sqrt[3]{2})$, which is crucial for this set to be a field.

We ended class constructing the multiplicative inverse of $4 + \sqrt[3]{2} + \sqrt[3]{4}$ in $\mathbb{Q}(\sqrt[3]{2})$.

Friday, March 22. We began by defining what a prime ideal and what a maximal ideal iis in a commutative ring R. After discussing why $\langle x, y\rangle$ is a maximal ideal in $\mathbb{Q}[x, y]$, we discusses and verified the following proposition.

Proposition. Let R be a commutative ring.

(i) An ideal $P \subseteq R$ is a prime ideal if and only if R/P is an integral domain.
(ii) An ideal $M \subseteq R$ is a maximal ideal if and only if R/M is a field.

We then defined a commutative ring to be *Noetherian* if it satisfies any one, and hence all, of the conditions in the next proposition.

Proposition. The following conditions are equivalent for the commutative ring R:

(i) R satisfies the *ascending chain condition*, i.e., given a chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there exists n_0 such that for all $n \geq n_0$, $I_{n_0} = I_n$.
(ii) R satisfies the *maximal condition*, i.e., any non-empty collection of ideals of R has a maximal element.
(iii) Every ideal of R is finitely generated.

We also noted that the Noetherian condition can be stated for non-commutative rings, but one must define the notions of *left Noetherian* and *right Noetherian* by restricting to left or right ideals in the previous proposition.

We then stated the celebrated:

Hilbert's Basis Theorem. Let R be a Noetherian commutative ring. Then $R[x]$, the polynomial ring in one variable over R, is Noetherian.

We ended clss by noting that two immediate consequences of the Hilbert Basis Theorem are that the polynomial rings $F[x_1, \ldots, x_n]$, with F a field, and $\mathbb{Z}[x_1, \ldots, x_n]$are Noetherian. Since a homomorphic image of a Noetherian ring is clearly Noetherian, it followed that homomorphic images of these polynomial rings are Noetherian, which implies that most of the rings encountered in algebraic geometry and algebraic number theory are Noetherian. In particular, since any Noetherian ring automatically satisfies the ascending chain condition on principal ideals, it follows that every non-zero, non-unit in a Noetherian domain can be factored as a product of irreducible elements, a fact that applies to the rings in algebraic geometry and algebraic number theory. However, such rings need not be UFDs - which shows that it is the *uniqueness of factorization* that eludes the non-UFDs encountered in algebraic geometry and algebraic number theory.

Wednesday, March 20. We worked through the details showing that $R := \mathbb{R}[x, y]/\langle x^2 + y^2 - 1\rangle$, is *not* a UFD. This fact follows because the image of x in R is an irreducible element that is not a prime element. Crucial steps in the proof required showing:

- (i) R is an integral domain. Here we used Eisenstein's criterion in the exact same way as in the previous lecture.
- (ii) $\overline{x}$, the image of x in R, is not a prime element. This followed since $R/\langle\overline{x}\rangle \cong \mathbb{R}[y]/\langle y^2 - 1\rangle$, which is not an integral domain.
- (iii) Every polynomial in $f \in \mathbb{R}[x, y]$ can be written uniquely as $f = f_0 + f_1 + \cdots + f_n$, where each $f_j \in \mathbb{R}[x, y]$ is homogeneous of degree j.
- (iv) $x^2 + y^2$ is an irreducible polynomial in $\mathbb{R}[x, y]$.
- (v) $\overline{x} \in R$ is an irreducible element.

For part (iv), we needed the following lemma:

Lemma. Suppose $f \in \mathbb{R}[x, y[$ is homogeneous of degree two and f is not irreducible. Then $f = gh$, where $g, h \in \mathbb{R}[x, y]$ are homogeneous of degree one. To see this, one writes $g = g_n + \cdots + g_0$ and $h = h_m + \cdots + h_0$, where each g_i, h_j are homogeneous of degrees i and j, and $n, m > 0$, and neither n nor m equal to 0. Then $0 \neq g_n h_m$ is the the largest homogeneous part of the product gh, so $n = m = 1$. Thus, $f = f_2 = g_1 h_1$, which gives what we want. Note, using that g_0 or h_0 must be zero, one can show $g = g_1$ and $h = h_1$, though this is not needed.

We then addressed the question: Why doesn't this same approach show that $S := \mathbb{C}[x, y]/\langle x^2 + y^2 - 1\rangle$ is not a UFD? The answer is that while the image of x in S is still not prime, the image of x in S is no longer irreducible. In fact, in S we have

$$x \equiv \frac{1}{2}(x - iy) \cdot \{(x + iy + i)(x + iy - i)\},$$

where $x - iy$ is a unit in S, but neither $x + iy + i$ nor $x + iy - i$ are units in S.

Monday, March 18. We worked through the details showing that the ring $R := \mathbb{C}[x, y]/\langle x^2 + y^2 - 1\rangle$ is a UFD. Crucial steps in the proof required showing:

- (i) If p is a prime element in the integral domain S, then $S/\langle p\rangle$ is an integral domain (and conversely).
- (ii) R is an integral domain. For this, we first proved Eisenstein's criterion and applied it to the polynomial $x^2 + y^2 - 1$.
- (iii) $R \cong \mathbb{C}[U, V]/\langle UV - 1\rangle$.
- (iv) $\mathbb{C}[U, V]/\langle UV - 1\rangle \cong \mathbb{C}[U, U^{-1}]$. This followed by showing that the ring homomorphism $\phi : \mathbb{C}[U, V] \to \mathbb{C}[U, U^{-1}]$ given by $\phi(f(U, V)) = f(U, U^{-1})$ is surjective with kernel equal to $\langle UV - 1\rangle$.

(iv) For an indeterminate U, the *Laurent polynomial ring* $\mathbb{C}[U, U^{-1}]$ is a UFD. This followed first by noting that $\mathbb{C}[U, U^{-1}] = \mathbb{C}[U]_S$, where $S = \{1, U, U^2, \dots, \}$ and invoking a property of localization, which is Problem 9 on Exam 2.

Friday, March 8. Group work on homework problems.

Wednesday, March 6. We continued along our path leading to the one of the main theorems in the course, namely, if R is a UFD, then $R[x]$ is a UFD. We began by recalling the quotient field of an integral domain as well as Proposition A and Gauss's Lemma from the previous lecture. We also observed that if R is a UFD with quotient field K, then any $h(x) \in K[x]$ can be written as $\frac{a}{b} \cdot h_0(x)$, where $a, b \in R$ have no common factor and $h_0(x) \in R[x]$ is a primitive polynomial. We then proceeded to prove the following two propositions.

Proposition B. Suppose R is a UFD with quotient field K and $f(x) \in R[x]$ is primitive. Then $f(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$.

Proposition C. Suppose R is a UFD and $f(x) \in R[x]$ is primitive and irreducible. Then $f(x)$ is a prime element.

After presenting these propositions we were able to give a proof of the following theorem.

Theorem. If R is a UFD, then $R[x]$, the polynomial ring in one variable over R, is also a UFD.

The idea behind the proof of the theorem was the following: Given $f(x) \in R[x]$ we may write $f(x) = af_0(x)$, where $a \in R$ and $f_0(x) \in R[x]$ is primitive. Since a can be factored as a product of primes, which remain prime in $R[x]$ (by Proposition A), it suffices to show that $f_0(x)$ is a product of primes in $R[x]$ and for this (by Proposition C), it suffices to show that $f_0(x)$ is a product of irreducible primitive polynomials in $R[x]$. This followed by factoring $f_0(x)$ as a product of irreducible polynomials in $K[x]$ and then using the observation stated in the first paragraph above together with Proposition B. We ended class by noting that, by induction, the following rings are UFDs: $F[x_1, \dots, x_n]$, F any field; $\mathbb{Z}[x_1, \dots, x_n]$; $R[x_1, \dots, x_n]$, for R a UFD.

Monday, March 4. We began with the construction the *quotient field* K of an arbitrary integral domain R, as described in Homework 16. We noted that (up to isomorphism) R can be identified with a subring of K and that K is the smallest field containing R, in the sense that K is contained in any field containing R.

We then began a discussion of the basic strategy for proving one of the main results of this part of the course, namely if R is a UFD, then $R[x]$ is a UFD. The idea is to use in tandem the facts that R is a UFD and $K[x]$ is a UFD, for K the quotient field of R. Illustrating the idea with the ring $\mathbb{Z}[x]$, we noted that $f(x) \in \mathbb{Z}[x]$ can be written as $af_0(x)$, where $a \in \mathbb{Z}$ and $f_0(x) \in \mathbb{Z}[x]$ has the property that there is no common divisor among the coefficients of $f_0(x)$. We then pointed out that on the one hand, we will show that the prime factorization of a in R remains a prime factorization of a as an element of $R[x]$, while on the other hand, the factorization of $f_0(x)$ in $K[x]$ as a product of irreducible polynomials is actually a factorization of $f_0(x)$ in $R[x]$ as a product of irreducible elements.

Before setting out on our path towards the proof of the theorem, we began with the following observation. For $0 \neq a \in$ and $f(x) \in R[x]$, $a \mid f(x)$ in $R[x]$ if and only if, in R, a divides every coefficient of $f(x)$. We then proved the following fact (one of many versions of Gauss's lemma):

Proposition A. For a UFD R, if $p \in R$ is a prime element, then p is also a prime element in $R[x]$.

We then defined $f(x) \in R[x]$ to be a *primitive* polynomial, if for all prime elements $p \in R$, $p \nmid f(x)$ in $R[x]$. This immediately gave rise to the following more common version of Gauss's lemma:

Gauss's lemma. *Let R be a UFD. Then the product of primitive polynomials is primitive.*

Friday, March 1. We began class by noting the following properties relating division of elements to containments of principal ideals. For an integral domain R:

(i) $a \mid b$ if and only if $\langle b \rangle \subseteq \langle a \rangle$.
(ii) $\alpha a \rangle = \langle b \rangle$ if and only if $b = au$, for some unit $u \in R$.
(iii) $q \in R$ is irreducible if and only $\langle q \rangle$ is maximal among principal ideals.
(iv) $p \in R$ is prime if and only if whenever $ab \in \alpha p \rangle$, $a \in \alpha p \rangle$ or $b \in \alpha p \rangle$.

We then proved the following sequences of propositions.

Proposition A. For an integral domain R, consider the following statements:

(i) R satisfies the ascending chain condition on principal ideals.
(ii) Every non-empty collection of principal ideals has a maximal element.
(iii) Every non-zero, non-unit in R is a product of finitely many irreducible elements.

Then statements (i) and (ii) are equivalent, and imply statement (iii).

Proposition B. Let R be a PID. Then R satisfies the ascending chain condition on principal ideals.

Proposition C. Let R be a PID. Then every irreducible element is a prime element.

We ended class by noting that the following theorem is an immediate consequence of Propisitions A, B, and C.

Theorem. Every PID is a UFD.

Wednesday, February 28. We continued our discussion of integral domains, by first reviewing the crucial definitions of *prime element* and *irreducible element*. We then gave a proof of the following

Proposition. *Let R be an integral domain. Then the following are equivalent:*

(a) Every non-zero, non-unit of R can be written as a product of prime elements.
(b) Every non-zero, non-unit in R can be written uniquely (up to order and unit multiples) as a product of irreducible elements.

We noted that a key point in the proof of the proposition was that irreducible elements are prime in the presence of either condition (a) or (b). We then defined a *Unique Factorization Domain*, or UFD, to be any ring satisfying the conditions of the previous proposition. We noted again that any ring with a division algorithm is a UFD, this includes such rings as $\mathbb{Z}, F[x]$ and the Gaussian integers $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$. We also indicated that the UFD properly is rather subtle by noting the following examples:

(i) The ring $\mathbb{R}[x, y]/\langle x^2 + y^2 - 1\rangle$ is not a UFD, while the ring $\mathbb{C}[x, y]/\langle x^2 + y^2 - 1\rangle$ is a UFD.
(ii) The ring $\mathbb{R}[x, y, z]/\langle x^2 + y^2 + z^2 - 1\rangle$ is a UFD, while the ring $\mathbb{C}[x, y, z]/\langle x^2 + y^2 + z^2 - 1\rangle$ is not a UFD.

This was followed by defining what it means for R to be a *Principal ideal Domain* (PID) and demonstrated how a ring with a division algorithm is a PID by proving that $F[x]$ is a PID for any field F. We also noted (but did not verify) the classical example of a ring which is a PID, but does not admit a division algorithm, namely $S := \{a + b\omega \mid a, b \in \mathbb{Z}\}$, where $\omega := \frac{1}{2} \cdot (1 + \sqrt{-19})$. We ended class by stating, but not proving that every PID is a UFD.

Monday, February 26. We began class by introducing the type of rings we will be studying for the next few weeks: A commutative ring R is said to be an *integral domain* (ID) if the product of non-zero elements is always non-zero. For example $\mathbb{Z}$ and $F[x]$, with F a field are examples of integral domains. We also noted that if R is an integral domain, then $R[x]$, the polynomial ring over R, is also an integral domain - since in this case, if $f(x), g(x) \in R[x]$, then the degree of $f(x)g(x)$ is the sum of the degrees of $f(x)$ and $g(x)$. We also noted that $\mathbb{Z}_6$ and the ring of continuous functions from $\mathbb{R} \to \mathbb{R}$ are **not** integral domains. This was followed by noting

Cancellation holds in an integral domains. Suppose R is an integral domain, and $a, b, c \in R$, with $a \neq 0$. If $ab = ac$, then $b = c$.

This was followed by giving a number of definitions for elements in an integral domain R, including the definitions of: $a \mid b$; a unit; associates; prime elements; irreducible elements. In particular, a non-zero, non-unit $p \in R$ is *prime* if whenever $p \mid ab$, $p \mid a$ or $p \mid b$ and $q \in R$ is an *irreducible element* if whenever $q = ab$, then a or b is a unit. We noted that primes are always irreducible, but irreducible elements need not be prime, an example being $3 \in \mathbb{Z} + \sqrt{-5}\mathbb{Z}$.

We ended class by proving the following proposition (whose conclusion was expected, based upon our proof of the uniqueness part of the Fundamental Theorem of Arithmetic) and discussing its relevance to a general theory of unique factorization

Proposition. Let R be an integral domain and $p_1, \dots, p_r q_1, \dots, q_t$ be primes in R. If $p_1 \cdots p_r = q_1 \cdots q_s$, then $r = s$ and after re-indexing, $q_i = p_i u_i$, for units u_i and $1 \le i \le r$.

Friday, February 23. Today's lecture was devoted to a discussion concerning, and a proof of:

Fundamental Theorem of Arithmetic. Every positive integer $n > 1$ can be written uniquely as as a product $n = p_1^{e_1} \cdots p_r^{e_r}$, where each p_i is prime and $e_i \ge 1$. Here uniqueness mens, if $n = q_1^{f_1} \cdots q_s^{f_s}$, with each q_j prime and $f_i \ge 1$, then $r = s$, and after re-indexing, we have $1 \le i \le r$, $q_i = p_i$ and $e_i = f_i$, for all $1 \le i \le r$.

The proof of the theorem required a few preliminary results:

(i) If $a, b \in \mathbb{Z}$, with $b > 0$, then there exist unique $q, r \in \mathbb{Z}$ such that $0 \le r < b$. (Division Algorithm).
(ii) Given $a, b \in \mathbb{Z}$, the greatest common divisor of a and b exists.
(iii) If $a, b \in \mathbb{Z}$ and $d = \mathrm{GCD}(a, b)$, then there exist $n, m \in \mathbb{Z}$ such that $d = ma + nb$. (Bezout's Principle)

The division algorithm was proven by finding a least positive integer r among all expressions of the form $a - bk$, with $k \in \mathbb{Z}$ and $a - bk \ge 0$. We then used the division alrgoithm to show (ii) and (iii), the key observation being if $a, b \in \mathbb{Z}$ with $b > 0$ and $a = bq - r$, with $0 \le r < b$, then the set of common divisors of a and b is the same as the set foc common divisors of b and r. We then used Bezout's principle to prove the following **important properties of primes**:

If $p, a, b \in \mathbb{Z}$, with p prime, and $p \mid ab$, then $p \mid a$ or $p \mid b$.

We then gave a proof of the Fundamental Theorem of Arithmetic, by first showing existence of a factorization. This followed by noting that if factorization failed, the set X of positive integers (greater than 1) not admitting a factorization would have a least element, say n. Since n would not be prime $n = ab$, with a, b positive integers less than n, and thus $a, b \notin X$. Therefore each of a, b have a prime factorization, and hence ab has a factorization, a contradiction forcing X to be empty. Uniqueness of factorization followed by induction and the important property of primes stated above.

We ended class by discussing how exactly the same steps used in proving the Fundamental Theorem of Arithmetic can be used to prove the following fact: For F a field, every monic polynomial $f(x) \in F[x]$ can be factored uniquely as a product $f(x) = p_1(x)^{e_1} \cdots p_r(x)^{e_r}$, with each $p_i(x)$ monic and irreducible over F. This works because $F[x]$ also has a (familiar) division algorithm.

Wednesday, February 21. We continued our discussion of rings in the abstract, beginning with a discussion concerning ideals in the ring R generated by the set $X \subseteq R$. We noted that if one defines the *left ideal of R generated by X*, denoted $\langle X \rangle_L$, to be the intersection of all left ideals of R containing X, then $\langle X \rangle_L$ equals the set of all finite expressions of the form $r_1 x_1 + \cdots + r_n x_n$, with each $r_i \in R$ and $x_i \in X$. We then defined the *right ideal of R generated by X* and the *two-sided ideal of R generated by X* in similar ways and noted that we have similar intrinsic descriptions.

We then showed that if $I \subseteq R$ is a two-sided ideal, the abelian group $(R/I, +)$ has a natural ring structure, where coset multiplication is defined as $(a + I) \cdot (b + I) := ab + I$. After defining what it means for a map $f : R \to S$ between rings to be a *ring homomorphism*, we noted that a subset $I \subseteq R$ is a two-sided ideal if and only if I is the kernel of a ring homomorphism. We then noted that one has essentially the same correspondence and isomorphism theorems for rings as for groups, in particular

(i) If $f : R \to S$ is a surjective ring homomorphism, then there is a one-to-one correspondence between the two-sided (resp., left or right) ideals of S and the two-sided (resp., left or right) ideals of R containing $\ker(f)$.
(ii) If $f : R \to S$ is a surjective ring homomorphism, then $R/\ker(f) \cong S$.
(iii) If $J \subseteq I \subseteq R$ are two-sided ideals then I/J is a two-sided ideal of R/J and $(R/J)/(I/J) \cong R/I$.

We ended class by discussing the Fundamental Theorem of Arithmetic for $\mathbb{Z}$ and some of its more subtle points, especially what uniqueness of factorization means when we factor a positive integer **uniquely** into a product of primes.

Monday, February 19. We began our discussion of ring theory by defining a (not necessarily commutative) ring as a set with two binary operations $+, \cdot$ such that:

(i) $(R, +)$ is an abelian group.
(ii) Multiplication is associative.
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$, for all $a, b, c \in R$.
(iv) R has a multiplicative identity, denoted as 1, satisfying $1 \cdot a = a = a \cdot 1$, for all $a \in R$.

We then gave several examples of rings, including $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$, rings of functions on a set taking values in a commutative ring, and matrix rings. This was followed by a discussion of various types of ideals in a ring: left ideals, right ideals, and two-sided ideals. Examples of each were given. We noted that for R, the ring of 2×2 matrices over $\mathbb{R}$:

(i) The set of matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ is a left ideal.
(ii) The set of matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ is a right ideal
(iii) The only non-zero two-sided ideal has to be the whole ring.

We also noted that if $R = \mathrm{M}_n(\mathbb{Z})$, then the matrices whose entries are even integers gives an example of a proper two-sided ideal in R. Similarly, $\mathrm{M}_2(n\mathbb{Z})$ is a two-sided ideal of R, for any $n \geq 2$. We ended class by noting that these are the only two-sided ideals in R.

Friday, February 16. Today's class was devoted to a proof of the following theorem.

Theorem. *Let G be a simple group of order 60. Then G is isomorphic to A_5.*

Proof. Suppose we could find a group homomorphism from G to S_5. Since G is simple, the kernel of this homomorphism is $\{e\}$. Thus, G is isomorphic to a subgroup $G' \subseteq S_5$. Since $|G'| = 60$, $[S_5 : G'] = 2$, so that G' is a proper normal subgroup of S_5. By problem 3 on Homework 8 or problem 7 on Exam 1, $G' = A_5$, so that G is isomorphic to A_5, as required.

Thus, we seek a group homomorphism $\psi : G \to S_5$. For this recall that such a homomorphism exists, if G acts on a set with 5 elements. We first note that $60 = 2^2 \cdot 3 \cdot 5$, so that any Sylow 2-subgroup has four elements, any Sylow 3-subgroup has three elements and any Sylow 5-subgroup has five elements. By the Third Sylow Theorem, for $p = 2, 3, 5$, the number of p-Sylow subgroups divides 60 and is congruent to 1 modulo p. Based upon this we have:

$$\text{Possible number of Sylow 2-subgroups} = 1, 3, 5, 15$$
$$\text{Possible number of Sylow 3-subgroups} = 1, 4, 10$$
$$\text{Possible number of Sylow 5-subgroups} = 1, 6$$

In each case, we can eliminate the possibility of one Sylow subgroup, for then that subgroup would be normal in G, contradicting the simplicity of G. Suppose we had four Sylow 3-subgroups. Then if G acts on the set of Sylow 3-subgroups via conjugation, and thus we would have a group homomorphism $\psi : G \to S_4$. Since $|S_4| = 24$, $\ker(\psi) \neq \{e\}$. But then G would have a non-trivial normal subgroup, which is a contradiction. Thus, G must have ten Sylow 3-subgroups. Now, by Lagrange's theorem, any two of the Sylow 3-subgroup have to intersect in $\{e\}$, since the intersection is a subgroup of each. Thus, there are $10 \cdot 2 = 20$ elements in G having order 3.

Since we cannot have one Sylow 5-subgroup, there must be six of them, and since they each have prime order, the intersection of any two of them must be $\{e\}$. Thus, there are $6 \cdot 4 = 24$ elements of order 5 in G. We have now accounted for $20 + 24 = 44$ elements of G.

Regarding the number of Sylow 2-subgroups, we cannot have just three of them, otherwise, there would exist a group homomorphism $\psi : G \to S_3$, which would necessarily have a non-trivial kernel. If the number of Sylow 2-subgroups equals five, then we let G act on the set of Sylow 2-subgroups via conjugation. This then gives a group homomorphism $\psi : G \to S_5$, which is what we want.

Suppose the number of Sylow 2-subgroups equals fifteen. First assume the following: Given any two such subgroups, say, P_1 and P_2, $P_1 \cap P_2 = \{e\}$. Then G would contain $15 \cdot 3 = 45$ elements of order two or four, which is a contradiction, since we already have 44 elements of order three or five. Thus, there must be at least two P_1, P_2 with $P_1 \cap P_2 \neq \{e\}$. Then $|P_1 \cap P_2| = 2$. If $e \neq x \in P_1 \cap P_2$, then since P_1 and P_2 are abelian, x commutes with every element in both P_1 and P_2. Thus, both P_1 and P_2 are contained in $C_G(x)$, the centralizer of x. Since $|P_1P_2| = 8$, and $P_1P_2 \subseteq C_G(x)$ (as sets), $|C_G(x)| \geq 8$ and $|C_G(x)|$ divides 60. Moreover, since $P_1 \subseteq C_G(x)$, 4 divides $|C_G(x)|$. Thus, $|C_G(x)| = 12$ or 20.

Suppose $|C_G(x)| = 12$. Then $[G : C_G(x)] = 5$. Thus, if we let G act on the set of left cosets of $C_G(x)$ in G via translation, there exists a group homomorphism $\psi : G \to S_5$, which is what we want. If $|C_G(x)| = 20$, then, in a similar way, there would exist $\psi : G \to S_3$, which would have non-trivial kernel, so this case does not exist. Thus, if the number of Sylow 2-subgroups equals fifteen, then the required map $\psi : G \to S_5$ exists and this completes the proof of the theorem. □

We ended class by noting that the proof does not actually show whether or not the simple group G has five or fifteen Sylow 2-subgroups, nor what those subgroups look like. Since G is isomorphic to A_5, it suffice to determine the Sylow 2-subgroups of A_5. We noted that A_5 has five Sylow 2-subgroups all isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. In fact, here are five Sylow 2-subgroups of A_5, all of which are isomorphic to $\mathbb{Z}\_2 \times \mathbb{Z}_2$:

$P_1 := \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$
$P_2 := \{id, (5,2)(3,4), (5,3)(2,4), (5,4)(2,3)\}$
$P_3 := \{id, (1,5)(3,4), (1,3)(5,4), (1,4)(5,3)\}$
$P_4 := \{id, (1,2)(5,4), (1,5)(2,4), (1,4)(2,5)\}$
$P_5 := \{id, (1,2)(3,5), (1,3)(2,5), (1,5)(2,3)\}$.

To see that there are no other Sylow 2-subgroups of A_5, note that since there are 44 elements in A_5 with order three or five, there must be fifteen elements with order two, and our list above accounts for fifteen elements of order two. We now note that there cannot be any other Sylow 2-subgroups. Suppose P were another Sylow 2-subgroup, say $P = \{id, u, v, w\}$. Then each of u, v, w must belong to different P_i, since if, for example, $u, v \in P_i$, then $w = uv \in P_i$ would yield $P = P_i$. Suppose $u = (a,b)(c,d) \in P_i$. In order for v to be in $P_j \neq P_i$, v must involve e and omit one of a, b, c, d. Without loss of generality, we assume v omits a. Here we are assuming $\{1,2,3,4,5\} = \{a,b,c,d,e\}$. Thus, v is one of $(e,b)(c,d), (e,c)(b,d), (e,d)(b,c)$. We therefore have one of the following three possibilities for $w = uv$:

$$(a,b)(c,d)(e,b)(c,d) = (a,b,e)$$
$$(a,b)(c,d)(e,c)(b,d) = (a,b,c,e,d)$$
$$(a,b)(c,d)(e,d)(b,c) = (a,b,d,e,c).$$

But each of these cases lead to a contradiction, since w has order two. Thus, there are five Sylow 2-subgroups of A_5, each isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Wednesday, February 14. We began by stating the three Sylow theorems. Here are the second and third Sylow theorem (the first Sylow theorem is stated in the previous update).

Second Sylow Theorem. *Let G be a finite group such that $|G| = p^n m$, where p is prime and p does not divide m. Suppose $H \subseteq G$ is a subgroup of order p^i, with $1 \leq i \leq n$ and P is a Sylow p-subgroup. Then there exists $a \in G$ such that $H \subseteq aPa^{-1}$. In particular, any two Sylow p-subgroups are conjugate.*

Third Sylow Theorem. *Let G be a finite group such that $|G| = p^n m$, where p is prime and p does not divide m and write n_p for the number of Sylow p-subgroups. Then n_p divides $|G|$ and is congruent to 1 mod p.*

We then gave applications of these theorems by showing any group of order 36 or 105 has a non-trivial normal subgroup, We then provided proofs of the second and third Sylow theorems. The proofs of these theorems relied on the following lemma:

Lemma. Let G be a group of order p^t, with p prime, and assume G acts on the finite set X. If r denotes the number of orbits with just one element, then $|X| \equiv r \pmod{p}$.

The proof of the second theorem followed by letting H act on X, the left cosets of some Sylow p-subgroup P, by left translation. We then used the Lemma to show that that $r \neq 0$. Thus, there exists $gP \in X$ such that $hgP = gP$, for all $h \in h$, so $hg \in gP$, for all $h \in H$, which gives $H \subseteq gPg^{-1}$. The third Sylow theorem followed by first letting G act on the set X of Sylow p-subgroups, so $n_p = |X|$, in this case. By the second

Sylow theorem, $\text{orb}(P) = X$, for any $P \in X$, so $n_p = |\text{orb}(P)|$ divides G. Then letting P act on X, we noted that P is the only element of X whose orbit has one element, so by the Lemma, $n_p = |X| \equiv 1 \pmod p$.

Monday, February 12. We stated and proved Cauchy's Theorem: If G is a finite group, and p is a prime dividing $|G|$, then G has an element of order p. Equivalently, G has a subgroup of order p, namely the cyclic subgroup generated by an element of order p. We then defined the notion of a Sylow p-subgroup for a finite group whose order is divisible by p. We then stated and proved:

First Sylow Theorem. *Let G be a finite group such that $|G| = p^n m$, where p is prime and p does not divide m. Then G has a Sylow p-subgroup. That is, there exists a subgroup $P \subseteq G$ such that $|P| = p^n$.*

The idea of the proof was the following: If $|G| = p$, the result is clear. Proceed by induction on $|G|$. Using the class equation, if p does not divide $|Z(G)|$, then p does not divide the index of some $C_G(x_i)$, where x_i is an element whose conjugacy class contains more than one element. It follows that p^n divides $|C_G(x_i)|$, so by induction, $C_G(x_i)$, and hence G, has a subgroup of order p^n. Otherwise, if p divides $|Z(G)|$, by Cauchy's theorem, there exists $x \in Z(G)$, with $o(x) = p$. One finishes the proof by applying induction to $G/\langle x\rangle$ and using the group correspondence theorem. We then recorded two consequences of this theorem:

(i) If $|G| = p^n m$, as in Sylow's theorem, then for each $1 \leq i \leq n$, there exist subgroups $H_1 \subseteq \cdots \subseteq H_n$ such that $|H_i| = p^i$.

(ii) If $|G| = pq^n$, with $p < q$ primes, then G has a normal Sylow q-subgroup (which is the unique Sylow q-subgroup).

The first statement follows from the Sylow theorem and the property proved in the previous lecture about groups of order p^n and the second statement follows from the Sylow theorem and the fact that a subgroup whose index is the smallest prime dividing the order of the group is normal.

Friday, February 9. Today the class did group work on homework problems.

Wednesday, February 7. We began class by recalling the basic ideas behind a group G acting on a set X, in particular, the important fact that if G acts on a set with n elements, then there is a group homomorphism fro G to S_n. This led to a discussion involving the *orbit* of $x \in X$, i.e., $\text{orb}(x) := \{g \cdot x \mid g \in G\}$ and the *stabilizer* of x, i.e., $G_x := \{g \in G \mid g \cdot x = x\}$. We also proved the:

Proposition. Assume the group G acts on the set X. Fix $x \in X$. The there is a 1-1, onto set map between $\text{orb}(x)$ and the set of distinct left cosets of G_x given by $g \cdot x \longrightarrow gG_x$. In particular, if $|\text{orb}(x)|$ or $[G : G_x]$ is finite, then $|\text{orb}(x)| = [G : G_x]$, and it follows that $|\text{orb}(x)|$ divides $|G|$, if G is finite.

We then noted that in the special case G acts on itself via conjugation, $\text{orb}(x) = \{gxg^{-1} \mid g \in G\}$, the *conjugacy class* of G and $G_x := \{g \in G \mid gx = xg\}$, the *centralizer* if X. We denoted the conjugacy class of x by $c(x)$ and the centralizer of x by $C_G(x)$. Thus, $|c(x))| = [G : C_G(x)]$, when either one of these is finite. We were thus led to a proof of the **very important**:

Class Equation. Let G be a finite group. Then:

$$\begin{aligned} |G| &= |Z(G)| + \Sigma_{i=1}^r |c(x_i)| \\ &= |Z(G)| + \Sigma_{i=1}^r [G : C_G(x_i)], \end{aligned}$$

where the sum is taken over the distinct conjugacy classes with more than one element. Here $Z(G)$ denotes the *center* of G, where $Z(G) := \{g \in G \mid gx = xg, \text{ for all } x \in G\}$.

Using the class equation, we were able to prove the following theorem.

Theorem. Let G be a finite group with $|G| = p^n$, with p prime and $n \geq 1$. Then:

(i) $Z(G) \neq \{e\}$

(ii) There is a sequence of subgroups $\{e\} \subsetneq H_1 \subsetneq H_2 \subsetneq \cdots \subsetneq H_{n-1} \subsetneq H_n = G$ such that each H_i is a normal subgroup of H_{i+1} and the quotient group $H_{i+1}/H_i \cong \mathbb{Z}_p$.

Part (i) followed immediately from the class equation, since each $[G : C_G(x_i)]$ divides p^n, while part (ii) follows by induction on n and the correspondence theorem from January 26 applied to $G/\langle y\rangle$, where $y \in G$ is an element of order p. We pointed out that the condition in (ii) means that G is a *solvable group.*

For future reference, here is the definition of solvable group in general.

Definition. The finite group G is said to be solvable if there is a sequence of subgroups of G,

$$\{e\} \subsetneq H_1 \subsetneq H_2 \subsetneq \cdots \subsetneq H_{n-1} \subsetneq H_n = G$$

such that each H_i is a normal subgroup of H_{i+1} and the quotient groups H_{i+1}/H_i are cyclic of prime order, or equivalently, the quotient groups H_{i+1}/H_i are abelian.

Monday, February 5. Given a set X and a group G, we defined what it means for G to *act* on X: There is a binary map $G \times X \xrightarrow{\cdot} X$ satisfying: (i) $e \cdot x = x$ and $(ab) \cdot x = a \cdot (b \cdot x)$, for all $a, b \in G$ and $x \in X$. We then discussed the following examples of group actions:

Examples Let G be a group and X a set:

(i) Taking $X = G$, then G *acts on itself via left translation*: $g \cdot x := gx$, for all $g \in G$ and $x \in X$.
(ii) If $H \subseteq G$ is a subgroup, and X denotes the set of distinct left cosets of H, then G *acts on* X *via left translation*: $g \cdot (aH) := gaH$, for all $g \in G$ and $aH \in X$.
(iii) $G = S_n$ acts on $X = \{1, 2 \ldots, n\}$, via $\sigma \cdot i := \sigma(i)$, for all $\sigma \in S_n$ and $i \in X$.
(iv) Taking $X = G$, then G *acts on itself via conjugation*: $g \cdot x := gxg^{-1}$, for all $g \in G, x \in X$.
(v) Suppose G has a subgroup of order n. If we let X denote the set of all subgroups of order n, then G *acts on* X *via conjugation*: $g \cdot H = gHg^{-1}$, for all $g \in G$ and $H \in X$.
(vi) If $G := \mathrm{Gl}_n(\mathbb{R})$ and $X := \mathbb{R}^n$, thought of as column vectors, then matrix multiplication defines a group action: $A \cdot v := Av$, for all $A|inG$ and $v \in X$.

We then observed that if G acts on X, then for fixed $g \in G$, the map $X \xrightarrow{\cdot g} X$ is one-to-one and onto. Thus, multiplication by g permutes the elements of X. This gave rise to the **very important**:

Proposition. If the group G acts on a set with n elements, then there is a group homomorphism $\phi : G \to S_n$.

The important point of the proposition is that the association between G and the elements of S_n is given by a group homomorphism. We also noted that the converse is left as a homework exercise, namely, if there is a group homomorphism $\phi : G \to S_n$, then ϕ induces a group action on any set with n elements. Hence: *To give an action of the group G on a set with n elements is equivalent to giving a group homomorphism from G to S_n.*

As an application of the previous proposition and a number of other results established, we then proved the following theorem.

Theorem. Let G be a finite group and $H \subseteq G$ a subgroup. Suppose $[G : H] = p$, where p is the smallest prime dividing the order of G. Then H is normal in G.

The ideal behind of the proof is there exists a group homomorphism $\phi : G \to S_p$ with kernel $K \subseteq H$. Thus, G/K is isomorphic to a subgroup of S_p and hence any prime q dividing $|G/K|$ divides $p!$. This forces $|G/K| = p$, which in turns gives $H = K$.

We finished class by noting that if G acts on the set X, and $x \in X$, then the *orbit of* x, denoted $\mathrm{orb}(x)$, is the set $\mathrm{orb}(x) := \{gx \mid g \in G\}$. We then showed that the distinct orbits of X form a partition of X.

Friday, February 2. After showing that the set $A_n$of even permutations forms a normal subgroup of index two in S_n, the rest of today's lecture was devoted to the proof of the following **very important theorem.**

Theorem. The alternating group A_n is a simple group for $n \geq 5$. In other words, there are no proper normal subgroups of A_n, for $n \geq 5$.

Proof. The proof proceeds in four steps.

Step 1. We first note that A_n is the subgroup of S_n generated by the set of all 3-cycles. To see this, if (u, v, w) is a 3-cycle, then $(u, v, w) = (u, w)(u, v)$, so that every 3-cycle belongs to A_n. Conversely, every element of A_n is a product of permutations of the form $(u, v)(s, t)$ or $(u, v)(u, s)$, for distinct elements $u, v, w, s \in X_n$. But, $(u, v)(s, t) = (u, s, v)(u, s, t)$ and $(u, v)(u, s) = (u, s, v)$, which shows that A_n is the subgroup of S_n generated by the set of 3-cycles.

Step 2. Fix $1 \leq a \neq b \leq n$. Then A_n is generated by the 3-cycles of the form (a, b, c) with $c \in X_n \backslash \{a, b\}$. To see this, let us note that any 3-cycle is of the form: $(a, b, u), (a, u, b), (a, u, v), (b, u, v), or (u, v, w)$, for a, b, u, v, w distinct elements of X_n. However, direct calculation shows that

$$\begin{aligned}(a, u, b) &= (a, b, u)^2 \\ (a, u, v) &= (a, b, v)(a, b, u)^2 \\ (b, u, v) &= (a, b, v)^2(a, b, u) \\ (u, v, w) &= (a, b, u)^2(a, b, w)(a, b, v)^2(a, b, u),\end{aligned}$$

which gives what we want.

Step 3. If N is a normal subgroup of A_n and N contains a 3-cycle, then $N = A_n$. To see this, let $(a, b, u) \in N$ be a 3-cycle. Then, by Step 2, it suffices to show that $(a, b, c) \in N$, for all $c \in X_n \backslash \{a, b\}$. However, using that $(a, b)(u, c)$ is its own inverse, we have

$$\{(a, b)(u, c)\}(a, b, u)^2\{(a, b)(u, c)\}^{-1} = (a, b)(u, c)(a, b, u)^2(a, b)(u, c) = (a, b, c),$$

which belongs to N since N is normal in A_n.

Step 4. If N is a normal subgroup of A_n, then N contains a 3-cycle. This is the hardest step, and requires consideration of several cases, where we analyze the decomposition of $\sigma \in N$ into a product of disjoint cycles.

Case (a). N contains an element σ of the form $\sigma := (i_1, \ldots, i_k)\tau$, where $k \geq 4$ and τ is a product of disjoint cycles, each of which is disjoint from $(i_1, \ldots, i_k)$. Set $\gamma := (i_1, i_2, i_3)$. Then $\sigma^{-1}(\gamma\sigma\gamma^{-1}) \in N$. However,

$$\sigma^{-1}(\gamma\sigma\gamma^{-1}) = \tau^{-1}(i_1, i_k, i_{k-1}, \ldots, i_2)(i_1, i_2, i_3)(i_1, \ldots, i_k)\tau(i_1, i_3, i_2) = (i_1, i_3, i_k),$$

which shows that N contains a 3-cycle.

Case (b). N contains $\sigma = (i_1, i_2, i_3)(i_4, i_5, i_6)\tau$, a product of disjoint cycles. Set $\gamma := (i_1, i_2, i_4)$. Then $\sigma^{-1}(\gamma\sigma\gamma^{-1}) \in N$. However,

$$\sigma^{-1}(\gamma\sigma\gamma^{-1}) = \tau^{-1}(i_4, i_6, i_5)(i_1, i_3, i_2)(i_1, i_2, i_4)(i_1, i_2, i_3)(i_4, i_5, i_6)\tau(i_1, i_4, i_2) = (i_1, i_4, i_2, i_6, i_3),$$

and thus, N contains a 5-cycle. By Case (a), N contains a 3-cycle.

Case (c). N contains $\sigma = (i_1, i_2, i_3)\tau$, where τ is a product of disjoint 2-cycles, disjoint from (i_1, i_2, i_3). Then $\sigma^2 \in N$, and since disjoint cycles commute,

$$\sigma^2 = (i_1, i_2, i_3)^2\tau^2 = (i_1, i_2, i_3)^2 = (i_1, i_3, i_2),$$

so N contains a 3-cycle.

Case (d). One of the previous three cases must hold. If not, then every element of N is a product of an even number of disjoint 2-cycles. Let $\sigma \in N$, and write $\sigma = (i_1, i_2)(i_3, i_4)\tau$ be the cycle decomposition of σ. Set $\gamma := (i_1, i_2, i_3)$, so that $\sigma^{-1}(\gamma\sigma\gamma^{-1}) \in N$. However,

$$\sigma^{-1}(\gamma\sigma\gamma^{-1}) = \tau^{-1}(i_3, i_4)(i_1, i_2)(i_1, i_2, i_3)(i_1, i_2)(i_3, i_4)\tau(i_1, i_3, i_2) = (i_1, i_3)(i_2, i_4).$$

For ease of notation, set $\alpha := (i_1, i_3)(i_2, i_4) \in N$.

Since $n \geq 5$, there exists $j \in X_n \backslash \{i_1, \ldots, i_4\}$. Set $\beta := (i_1, i_3, j) \in A_n$. Then, $\alpha\beta\alpha\beta^{-1} \in N$. However,

$$\alpha\beta\alpha\beta^{-1} = (i_1, i_3)(i_2, i_4)(i_1, i_3, j)(i_1, i_3)(i_2, i_4)(i_1, j, i_3) = (i_1, i_3, j),$$

showing that N contains a 3-cycle. But this is a contradiction, because any 3-cycle is the product of two 2-cycles that are *not* disjoint.

All possibilities for cycle decompositions that can occur have been covered by the cases above, thus N must contain a 3-cycle. It follows immediately from Steps 1,2,3 that A_n cannot have a proper, normal subgroup, and therefore, A_n is a simple group. □

Wednesday, January 31. We reviewed some of the properties of elements in S_n, in particular, we showed that for a k-cycle $\sigma \in S_n$ and a fixed $i \in X_n$:

(i) There exists a least positive integer $s \geq 1$ such that $\sigma^s(i) = i$.
(ii) $\{\sigma^n(i) \mid n \in \mathbb{Z}\} = \{i, \sigma(i), \ldots, \sigma^{s-1}(i)\}$.

We then presented the following theorem.

Theorem. Let $\sigma \in S_n$. Then:

(i) σ can be written uniquely (up to order) as a product of disjoint cycles.
(ii) σ can be written as a product of (not necessarily disjoint) 2-cycles.

After this we then proved the theorem stating that no permutation in S_n can be written as a product of an even number of 2-cycles on the one hand, and a product of an odd number of 2-cycles on the other hand. The proof was based upon the following. Any $\sigma \in S_n$ corresponds to a matrix A_σ obtained by permuting the rows of the $n \times n$ identity matrix according to σ. In other words, if $R_1, \ldots, R_n$ are the rows of the identity matrix, then $R_{\sigma(1)}, \ldots, R_{\sigma(n)}$ are the rows of A_σ. We then showed that for any $\sigma, \tau \in S_n$, $A_\tau A_\sigma = A_{\sigma\tau}$. For the sake of completeness, here is a proof of this latter fact: We first note that the ith row of A_σ has all entries equal to zero, except 1 in the $\sigma(i)$th columns. Working over $\mathbb{Q}$, say, it follows that $A_\sigma \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_{\sigma(1)} \\ \vdots \\ a_{\sigma(n)} \end{pmatrix}$.

Now set $b_i := a_{\sigma(i)}$, for all $1 \le i \le n$. Then for $\tau \in S_n$, we have

$$A_\tau A_\sigma \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = A_\tau \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} b_{\tau(1)} \\ \vdots \\ b_{\tau(n)} \end{pmatrix} = \begin{pmatrix} a_{\sigma(\tau(1))} \\ \vdots \\ a_{\sigma(\tau(n))} \end{pmatrix} = A_{\sigma\tau} \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Since this holds for all vectors $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, it follows that $A_\tau A_\sigma = A_{\sigma\tau}$.

From this, one has if $\sigma \in S_n$ and $\sigma = \tau_1 \cdots \tau_r = \gamma_1 \cdots \gamma_s$, where each τ_i, γ_j is a 2-cycle, then, on the one hand,

$$\begin{aligned} \det(A_\sigma) &= \det(A_{\tau_1 \cdots \tau_r}) \\ &= \det(A_{\tau_r} \cdots A_{\tau_1}) \\ &= \det(A_{\tau_r}) \cdots \det(A_{\tau_1}) \\ &= (-1)^r \end{aligned}$$

while on the other hand,

$$\begin{aligned} \det(A_\sigma) &= \det(A_{\gamma_1 \cdots \gamma_s}) \\ &= \det(A_{\gamma_s} \cdots A_{\gamma_1}) \\ &= \det(A_{\gamma_s}) \cdots \det(A_{\gamma_1}) \\ &= (-1)^s. \end{aligned}$$

Thus, $(-1)^r = (-1)^s$, which shows that both r and s are even, or both r and s are odd.

Monday, January 29. We spent most of the class discussing and proving the following isomorphism theorems.

First Isomorphism Theorem. Let $\phi : G_1 \to G_2$ be a surjective group homomorphism with kernel K. Then $G_1/K \cong G_2$.

Second Isomorphism Theorem. Let $K \subseteq N \subseteq G$ be groups such that K and N are normal in G. Then N/K is a normal subgroup of G/K and $(G/K)/(N/K) \cong G/N$.

After proving these theorems, we began a discussion of the structure of elements in the symmetric group S_n. We started with the definition of a k-cycle: $\tau \in S_n$is a k-cycle if there exists $i_1, \ldots, i_k \in X = \{1, 2, \ldots, n\}$ such that $\tau(i_1) = i_2, \tau(i_2) = i_3, \ldots, \tau(i_{k-1}) = i_k, \tau(i_k) = i_1$, and $\tau(j) = j$, if $j \notin \{i_1, \ldots, i_k\}$. We first observed that the order of a k-cycle is k. We then showed that disjoint cycles commute. We then stated the property that if τ is a k-cycle and γ is an s-cycle, and these cycles are disjoint, then the order of $\gamma\tau$ is the least common multiple of k and s.

We ended class by stating the important fact that every permutation in S_n is a product of disjoint cycles.

Friday, January 26. After recalling some basic consequences of the definition of group homomorphism, we spent the rest of the lecture proving the following theorem and its corollaries.

Theorem. Let $\phi : G_1 \to G_2$ be a surjective group homomorphism with kernel K. Then there is a one-to-one, onto correspondence between the subgroups of G_1 containing K and the subgroups of G_2 given by $H \longrightarrow \phi(H)$, for $H \subseteq G_1$ containing K, and $L \longrightarrow \phi^{-1}(L)$, for $L \subseteq G_2$. Under this correspondence, $\phi(H)$ is normal in G_2, if H is normal in G_1 and $\phi^{-1}(L)$ is normal in G_1, if L is normal in G_2.

Our first corollary noted that exactly the same theorem holds for ϕ not necessarily surjective if we replace G_2 by $\mathrm{im}(\phi)$. We then discussed at length the following corollary.

Corollary. Let G be a group and N a normal subgroup. Then there is a one-to-one, onto correspondence between the subgroups of G containing N and the subgroups of G/N. Under this correspondence, the normal subgroups of G containing N correspond to the normal subgroups of G/N.

We noted that this corollary follows from the theorem by taking $\phi : G \to G/N$ to be $\phi(g) = gN$, for all $g \in G$. In particular, we saw that any subgroup of G/N is necessarily of the form H/N, for H a subgroup of G containing N.

Wednesday, January 24. We began class with restating the equivalent conditions for a subgroup $N \subseteq G$ to be normal and noting important observation that if N is a normal subgroup of the group G, then for all $g \in G$ and $n \in N$, there exists $n' \in N$ such that $gn = n'g$. In other words, in the product gn we can move g passed n, at the expense of changing n to n'. We then showed that G/N - the set of left cosets of N - forms a group under coset multiplication by showing the product $g_1Ng_2N = g_1g_2N$. The resulting group is called the *quotient, or factor, group* of G by N, often referred to as *G mod N*. We then calculated group tables for various quotient groups, including $\mathbb{Z}/2\mathbb{Z}$ and Q_8/K, for $K = \{\pm 1\}$.

We followed this by a general discussion of how one might try to better understand the structure of a group G by considering a normal subgroup $N \subseteq G$ and the factor group G/N. This lead to a very informal discussion about simple groups and the history of the classification of finite simple groups.

We then defined the concept of a *group homomorphism*: The function $\phi : G_1 \to G_2$ is a group homomorphism if $\phi(ab) = \phi(a)\phi(b)$, for all $a, b \in G_1$. We noted (but did not prove) that $\phi(e_1) = e_2$ and $\phi(g^{-1}) = \phi(g)^{-1}$, for all $g \in G$. This was followed by defining the *kernel* of ϕ to be the set $\ker(\phi) := \{g \in G_1 \mid \phi(g) = e_2\}$. We ended class by noting, but not proving the following:

Proposition. Let $\phi : G_1 \to G_2$ be a group homomorphism, with kernel K. Then K is a normal subgroup of G_1. Conversely, any normal subgroup of G_1 is the kernel of a group homomorphism whose domain is G_1. Thus, normal subgroups are exactly kernels of group homomorphisms.

Monday, January 22. We began class by recalling the definitions of left and right cosets and also that if H is a subgroup of G, and $g_1, g_2 \in G$, then either $(g_1H) \cap (g_2H) = \emptyset$ or $g_1H = g_2H$. We then noted that for any $g \in G$, there is a 1-1, onto set function $\phi : H \to gH$. This shows that if $|H| < \infty$, then $|gH| = |H|$. This lead immediatley to:

LaGrange's Theorem. Let G be a finite group and $H \subseteq G$ a subgroup. Then

$$\begin{aligned} |G| &= |H| \cdot (\text{number of distinct left cosets of } H) \\ &= |H| \cdot (\text{number of distinct right cosets of } H). \end{aligned}$$

It followed that for a finite group G, the number of distinct left cosets of H equals the number of distinct right cosets of H, which we defined to be the *index of H in G*, denoted $[G : H]$. We followed this by a discussion of normal subgroups, using the definition N is normal in G if and only if for all $g \in G$, $gN = Ng$. We then noted (but did not prove) the equivalent conditions from Homework 2.

Examples. We then gave the following list of examples of normal subgroups:

(a) Any subgroup of an abelian group.

(b) Every subgroup of the quaternion group $Q_8 := \{\pm 1, \pm i, \pm, j, \pm k\}$, though Q_8 is not abelian.
(c) The subgroup of S_3 generated by the 3-cycle $(1, 2, 3)$.
(d) Any subgroup of index two.
(e) For $G := \mathrm{Gl}_n(\mathbb{R})$, $N = \mathrm{Sl}_n(\mathbb{R})$, i.e., the set of $n \times n$ matrices over $\mathbb{R}$ with determinant one, is a normal subgroup G.

We ended class by stating, but not proving, the following theorem.

Theorem. Let G be a group and $H \subseteq G$ a subgroup. Assume that $[G : H]$ is the smallest prime dividing the order of $|G|$. Then H is normal in G.

Friday, January 19. We began with the definition of a subgroup H of a group G: A subset $H \subseteq G$ is a *subgroup* if : (i) H is closed under the binary operation of G and (ii) $h \in H$ implies $h^{-1} \in H$. It followed easily from this that H is a group in its own right under the binary operation of G. We then gave several examples of subgroups, including: $n\mathbb{Z} \subseteq \mathbb{Z}$; $\mathbb{Z} \subseteq \mathbb{Q}$; $\mathrm{Sl}_n(\mathbb{R}) \subseteq \mathrm{Gl}_n(\mathbb{R})$. Most importantly, we gave the following definition:

Definition. Let $X \subseteq G$ be a subset. Then the *subgroup of G generated by X*, denoted by $\langle X \rangle$, is the set of all finite expressions of the form $x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$, where each $x_i \in X$ and $\epsilon \in \{\pm 1, 0\}$.

We quickly noted that, in fact, $\langle X \rangle$ is a subgroup of G. We also stated, but did not prove, that $\langle X \rangle$ is the intersection of the subgroups of G containing X. An important case is when $X := \{a\}$ consists of a single element. In this case we refer to $\langle a \rangle$ as the *cyclic subgroup of G generated by a.*

Given a subgroup $H \subseteq G$, we defined the *left coset* $gH := \{gh \mid h \in H\}$, for any $g \in G$. Right cosets were defined similarly: $Hg := \{hg \mid h \in H\}$. We then showed that left congruence modulo H gives rise to an equivalence relation on G whose equivalence classes are just the left cosets of H in G. Here, we defined $a \equiv_l b \ (\mathrm{mod} H)$ to mean $b^{-1}a \in H$. It followed that for any two left (or right) cosets g_1H, g_2H, either $g_1H = g_2H$ or $(g_1H) \cap (g_2H) = \emptyset$. This immediately implied that the distinct left (respectively, right) cosests of H in G partition G.

We ended class by explicitly calculating several cosets in S_3. Using the notation from the previous lecture, we set $H := \langle \sigma \rangle$ and $K := \langle \tau \rangle$. Then we calculated $eH, \tau H$, and $\sigma\tau H$, noting that $\tau H = H\tau$, $\tau H = \sigma\tau H$, and that $H, \tau H$ are the distinct left cosets of H. We then calculated σK, $\sigma^2 K$, and $K\sigma$, noting that, not only is $\sigma K \neq K\sigma$, but also that the right coset $K\sigma$ is not equal to any of the left cosets of K in G.

Wednesday, January 17. We began by recalling the definition of a group (and an abelian group) and gave several examples of groups, including: $\mathbb{Z}, \mathbb{Z}_n$ under addition, $\mathbb{Z}_n^*$ under multiplication, where the elements of $\mathbb{Z}_n^*$ are the residue classes of elements in $\mathbb{Z}$ relatively prime to n. We also defined S_n, the symmetric group on n objects and D_n, the dihedral group with $2n$ elements and $\mathrm{Gl}_n(\mathbb{R})$, the $n \times n$ invertible matrices over $\mathbb{R}$.

We defined S_n to be the set of 1-1, onto functions from the set $X := \{1, 2, \ldots, n\}$ to itself, with composition as the group operation. D_n was informally defined as the group of symmetries of a regular n-sided polygon, and we noted, but did not prove, that D_n is generated by a reflection about an axis of symmetry and a rotation of $\frac{2\pi}{n}$ radians clockwise about the center of the polygon, and all possible products of these two symmetries. It followed that $|S_n| = n!$ and $|D_n| = 2n$. We then introduced the notation $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ for elements of S_n, meaning that $\sigma(j) = i_j$, for $1 \leq j \leq n$, and used this notation to calculate all of the elements of S_3. In particular, taking $\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\tau := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, we calculated the products $\sigma^2, \sigma\tau, \sigma^2\tau$, noting that $\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ are the six distinct permutations of $\{1, 2, 3\}$ and thus $S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. We then noted that one can calculate all possible products of elements from S_3 by using the identities $\sigma^3 = e = \tau^2$ and $\tau\sigma = \sigma^2\tau$.

We ended class by noting, but not proving, that the identity element in an arbitrary group is unique and inverses in an arbitrary group are unique.