MATH 5550 - Abstract Algebra Lecture Notes 1

Libao Jin (ljin1@uwyo.edu)

May 7, 2017

Contents

1 Introduction and some concepts **1**
1.1 Binary operation . . . 1
1.2 Group . . . 1

2 Chapter 3 **8**
2.1 Group homomorphism . . . 8

3 Sylow Subgroups **14**
3.1 finite p-groups . . . 16

4 Permutation groups **17**

5 Chapter 7 Direct product **19**

6 Rings and Ideals **21**

7 Chapter 16: Commutative rings **26**

8 Fields **30**

1 Introduction and some concepts

1.1 Binary operation

- A binary operation $*$ on a set A is a function from $A \times A \to A$, written as $*(x, y)$, usually write $x * y$.
- **Punctilliation of** $\mathbb{Z}$: $x \star y = x^3 + xy - (x+1)^2$.
- Interesting properties a binary operation could have:
  - Commutativity (like $a * b = b * a$).
  - Associativity (like $(a * b) * c = a * (b * c)$).
  - Identity: element $e \in A$ with $e * x = x * e = x$.
  - Inverses: if $x \in A$, and $xy = yx = e$, we say y is an inverse of x.
- Example:
  1) A = set of all finite sequences of letters (standard English alphabets) including empty sequence, operation $*$ is concatenation: $(acu) * (juw) = acujuw$. It has associativity, and the identity is the empty sequence, but it does not have commutativity and inverses.
  2) $\odot$ on $\mathbb{R}$ defined by $x \odot y = xy + 1$. We can conclude that it has commutativity, but it does not have associativity since $0 \odot (0 \odot 1) = 1$ and $(0 \odot 1) \odot 1 = 2$. Assume it has identity e, so $e = 1 - \frac{1}{y}$, which depends on y, hence it is not an identity, as a result, it does not have inverses.
  3) $x \diamond y = x + y + 1$ on $\mathbb{R}$. It has commutativity and associativity. The identity $e = -1$, and the inverse of y is $-y - 2$.

1.2 Group

- A group is a set G with a binary operation $\circ$ satisfying:

  1) $\circ$ is associative.
  2) $\circ$ has an identity.
  3) every element of G has an inverse.

- Define the function g from $\{A, B, C, D\} \to \{A, B, C, D\}$: rotation by 90° counterclockwise (CCW).

$$\begin{cases} g : A \to D \to C \to B \to A \\ g^2 : A \leftrightarrow C, D \leftrightarrow B (180° \text{rotation}) \\ g^3 : A \to B \to C \to D \to A (270° \text{ CCW or } 90° \text{ CW}) \\ e : A \to A, B \to B, C \to C, D \to D. \end{cases}$$

  $g^4 = e$. Now let's define reflection:

$$\begin{cases} d : A \leftrightarrow C \\ k : B \leftrightarrow D \\ h : A \leftrightarrow D, B \leftrightarrow C \\ v : A \leftrightarrow B, D \leftrightarrow C \end{cases}$$

  Now let's define the function composition as a binary operation $\circ$. **Note:** $(x)f = f(x)$**,** $(g \circ f)(x) = f(g(x)) = x^{gf}$**.** Hence, we have $g \circ h : B \leftrightarrow D \Rightarrow g \circ h = k$. Hence, we have $G = \{e, g, g^2, g^3, h, gh, g^2h, g^3h\}$, where $g^4 = e$, $hg = g^3h$, $h^2 = e$.

- **Dihedral group**. D_{2n}: symmetries of regular n-gon.

  – Rotation: g by $\left(\frac{360}{n}\right)^\circ$.
  – Reflection: h through two fixed opposite vertices.
  – $D_{2n} = \{e, g, g^2, \cdots, g^{n-1}, h, gh, g^2h, \cdots, g^{n-1}h\}$, where $g^n = e$, $h^2 = e$, $hg = g^{n-1}h$. Presentation: $\langle g, h | g^n = e, h^2 = e, hg = g^{n-1}h \rangle$ ($\langle$ generator | relation $\rangle$).

- **Group**: A set G with a binary operation $\circ$ and an element $e \in G$ such that

  1) $x \circ e = e \circ x = x$.
  2) For all $x \in G$, there is a $y \in G$ with $xy = yx = e$.
  3) $\circ$ is associative.

- **Examples**

  1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under $+$.
  2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under $\cdot$.
  3) Dihedral group: D_{2n}.
  4) $GL(n, \mathbb{C})$: group of all invertible $n \times n$ complex matrices under matrix multiplication.
  5) $\mathbb{Q}_8 = \langle i, j, k, -1 | i^2 = j^2 = k^2 = -1, ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j \rangle = \{\pm i, \pm j, \pm k, \pm 1\}$.

- **Symmetric group**: Let X be a nonempty set $\mathrm{Sym}(X)$ is the group of all permutations of X (bijection from X to X) with the operation of function composition. $|\mathrm{Sym}(X)| = n!$, where $n = |X|$, if $n < \infty$.

- **Permutation group**: subgroup of $\mathrm{Sym}(X)$.

- **Cyclic group**: one generator and one relation (finite) or no relation (infinite).

$$\begin{cases} \langle g | g^n = e \rangle, & \text{if finite,} \\ \langle g | ... \rangle = \{e, g, g^2, \ldots, g^{-1}, g^{-2}, \ldots\}, & \text{if infinite (countably many)} \end{cases}$$

  1) $\mathbb{Z}/n\mathbb{Z}$: arithmetic (addition) mod n on congruence classes $\mathbb{Z} (\mathrm{mod}\, n)$, which is a finite cyclic group.
  2) $\mathbb{Z}$ under $+$ is an infinite cyclic group.

- **Lemma 1.5**: Let G be a group and let $a, b \in G$. Then there are unique solutions to the equation $\begin{cases} ax = b \\ ya = b \end{cases}$.

  Proof. Let a, b be as given. Since G is a group, there is a $z \in G$ with $az = za = e$. Then $x = zb$ satisfies $ax = b$, since $ax = a(zb) = (azb) = eb = b$. Similarly, $y = bz$ satisfies $ya = b$. To show uniqueness, since $ax' = b$ for some $x' \in G$. Then $ax = ax'$, so $z(ax) = z(ax') \Rightarrow (za)x = (za)x'$ giving $x = x'$.

- **Corollary**: The identity of a group is unique. The inverse of an element $x \in G$ is also unique.
- The inverse of x denoted as x^{-1} under multiplication while $-x$ under addition.
- Are $\mathbb{Z}/2\mathbb{Z}$ and $\langle g | g^2 = e \rangle$ same in the sense of group? Yes! $(\theta(x + y) = \theta(x)\theta(y))$
- **Isomorphism**: Let G, H be groups. The function $\theta : G \to H$ is an isomorphism provided that θ is a bijection and $\theta(xy) = \theta(x)\theta(y)$.
  - To show G is isomorphic to H, construct an isomorphism.
  - If it is not, find the difference of the structure, e.g. $\mathbb{Z}/8\mathbb{Z}$ is abelian (commutative) while D_8 is non-abelian. Hence, they are not isomorphic to each other.
  - Rotational symmetries of a cube: 24 symmetries. Is this isomorphic to D_{24}? (exercise)
- **Cayley's theorem**: G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

  Proof. For $x \in G$, define $r_x : G \to G$ by $r_x : g \mapsto gx$. (right-regular action)
  - We claim r_x is a permutation of G.
  - We next claim $R = \{r_x : x \in G\}$ is a group under function composition.

  $i_G = r_e$, so R has an identity. Also, $r_x \circ r_y = r_{xy} \in R$, so R is closed under $\circ$. Then $r_x \circ r_{x^{-1}} = r_{x^{-1}} \circ r_x = r_e$, so every element of R has an inverse. Therefore, R is a subgroup of $\mathrm{Sym}(G)$.
- Group G, $R = \{r_x : x \in G\} \leq \mathrm{Sym}(G)$. Define $\theta : G \to R$ via $\theta(x) = r_x$. Clearly, θ is sujective. To show injective, suppose $\theta(x) = \theta(y)$. Then $r_x(g) = r_y(g)$, $\forall g \in G$, so $gx = gy$, which implies $x = y$. Lastly, $\theta(xy) = r_{xy} = r_x \circ r_y$.
- **Example**: $D_8 = \{e, g, g^2, g^3, h, gh, gh^2, gh^3\}$. Let r_g be $e \to g, g \to g^2, g^2 \to g^3, g^3 \to e, h \to g^3h, gh \to h, g^2h \to gh, g^3h \to g^2h$.
- Isomorphism is an equivalence relation on groups. $G \cong H$: "G is isomorphic to H" or "There is an isomorphism from G to H".
- Relation:
  - reflective: $G \cong G$.
  - symmetric: $G \cong H \Leftrightarrow H \cong G$. (Because inverse θ^{-1} is also an isomorphism.)
  - transitive: if $G \cong H$, $H \cong K$, then $G \cong K$. (Composition of isomorphism is an isomorphism.)
- Rotational symmetries of a cube v.s. D_{24}.
  - Rotational symmetries of a cube: at least 8 of order 3.
  - D_{24}: only 2 of order 3.
- Define: Let $g \in G$. The order of g is the smallest natural number n satisfying $g^n = 1$. If no such n exists, we say the order of g is ∞.
- **Lemma**: Let $H \subseteq G$, $H \neq \emptyset$. Then H is a subgroup of G if and only if for all $x, y \in H$, xy^{-1} is also in H.

  Proof. $(\Rightarrow)$ If H is a subgroup of G, and $x, y \in H$, then $y^{-1} \in H$, so xy^{-1} must be in H.

  $(\Leftarrow)$ Suppose for all $x, y \in H$, $xy^{-1} \in H$. The operation of H is the same as that of G, so it is associative. Since H is nonempty, there is an $x \in H$. Then $xx^{-1} \in H$, so $e \in H$. Lastly, since $x, e \in H$, $ex^{-1} = x^{-1} \in H$.
- **Corollary 2.3**: Let $\mathcal{H}$ be a collection of subgroups of G. Then $D = \bigcap_{H \in \mathcal{H}} H$ is a subgroup of G.
- Subgroups generated by subsets. Given $X \subseteq G$, we define $\langle x \rangle$ to be the smallest (inclusion) subgroup of G containing X. $X = \{x_1, x_2, \ldots\}$, $e, x^{-1}, x_2^{-1}, \ldots$ and product of them are in the group generated by X.

- Convention: $\langle \emptyset \rangle = \{1\}$.
- We can also think of $\langle x \rangle$ as the set of all finite products $u_1, \ldots, u_t, t \in \mathbb{N}$, where u_i or $u_i^{-1} \in X$.
- **Example**: D_8: $\langle g \rangle$, $\langle h \rangle = \{1, h\}$, $\langle g^2, h \rangle = \{1, g^2, h, g^2h\}$ Given a group G and $g \in G$, look at structure of $\langle g \rangle$.
- **Corollary 2.5**: $\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$ (Cyclic group).
- **Lemma 2.6**: Let $G = \langle g \rangle$ and $H \neq \{1\}$ a subgroup of G. Let $g^n \in H$ be the smallest natural number such that

  (a) $g^m \in H$ if and only if $n|m$ (n divides m).
  (b) $H = \langle g^n \rangle$.

  Proof. (a) If $n|m$, clear. Conversely, suppose $g^m \in H$. Using the division algorithm, $m = ng + r, 0 \leq r < n$. Since $g^m, g^n \in H$, $g^m(g^{-n})^q \in H$, so $g^r \in H$. By the minimality of n, r must be 0. Therefore, $n|m$. (b) follows from (a).
- **Corollary 2.7**: Subgroup of cyclic groups are cyclic.
- **Lemma 2.8**: Let $g \in G$, $\sigma(G) = n < \infty$.

  (a) $g^m = 1$, if and only if $n|m$.
  (b) $g^m = g^l$, if and only if $m \equiv l (\mathrm{mod}\, n)$.
  (c) $|\langle g \rangle| = n, \langle g \rangle = \{1, g, \ldots, g^{n-1}\}$.
- A cyclic group is a group of the form $\langle g \rangle$, $G = \langle g \rangle, g^n \in H$.
- **Correction: Lemma 2.6**: H can be equal to $\{1\}$.
- Catch: If $|G|$ is infinite and $H = \{1\}$ then no such n exists.
- $G = \{1, g, g^2, g^3, g^4, g^5\}$, $H = \{1\}$, pick $n = 6, g^6 = 1 \in H$.
- **Lemma 2.8**: Let $g \in G$, $\sigma(g) = n < \infty$,

  (a) $g^m = 1$ iff. $n|m$.
  (b) $g^m = g^l$ iff. $m \equiv l (\mathrm{mod}\, n)$.
  (c) $|\langle g \rangle| = n$.

  Proof. (a)Follows from 2.6 (a) using $H = \{1\}$.

  (b) $g^m = g^l$ if and only if $g^{m-l} = 1$ if and only if $n|(m-l)$. This is equivalent to $m \equiv l (\mathrm{mod}\, n)$.
  (c) Every power of g is equal to one of $g, g^2, \ldots, g^{n-1}$ by b. Futhermore, these must all be distinct (again by (b)). Therefore $|\langle g \rangle| = n$.
- **Theorem 2.9**: Let G be a finite order cyclic group of order n. Then G has exactly one subgroup of order d for each $d|n$.
- Given $d|n$, $G = \langle g \rangle$, a subgroup of G of order d is given by $\langle g^{n/d} \rangle$.
- **Euler's totient function** $\phi(n)$: Let $u_n = \{r \in \mathbb{Z} | 0 \leq r < n, \gcd(n, r) = 1\}$. Define $\phi(n) = |u_n|$ (on domain $\mathbb{N}$).
- **Example**: $\phi(1) = 1$, $\phi(5) = 4$.
- If p is prime, $\phi(p) = p - 1$, $\phi(p^a) = p^a - p^{a-1}, a \in \mathbb{N}$.
- If the $\gcd(a, b) = 1$, then $\phi(a, b) = \phi(a)\phi(b)$.
- **Example**: $\phi(100) = \phi(4)\phi(25) = (4 - 2) \cdot (25 - 5) = 40$.
- **Theorem 2.10**: Let G be cyclic of order n, $G = \langle g \rangle$. Then G contains $\phi(n)$ elements of order n.

  Proof. Let $r \in \{0, \ldots, n-1\}$ and suppose $\gcd(r, n) > 1$. Then $d = \frac{n}{\gcd(r,n)} < n$, and $n|rd$. So $\sigma(g^r) \leq d$, since $(g^r)^d = 1$. Therefore $\sigma(g^r) < n$. Suppose $\gcd(r, n) = 1$. Let f be the least positive integer satisfying $g^f \in \langle g^r \rangle$. Then $f|r$. We also know that $g^n = 1 \in \langle g^r \rangle$, so $f|n$. Then f must be 1, so $\langle g^r \rangle = \langle g \rangle$ implying $\sigma(g^r) = n$. Therefore the number of elements of order n in G is $\phi(n)$.

- **Corollary**: Let G be a cyclic group of order n. Then G has exact $\phi(d)$ elements of order d for each $d|n$ and 0 if $d \nmid n$.

  Proof. For each $d|n$, there is a unique subgroup of order d which has exactly $\phi(d)$ elements of order d. And any elements of order d must generate a subgroup of order d. So there are no others.

- **Corollary**: $\sum_{d|n} \phi(d) = n$.

- **Example**: $\sum_{d|10} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$.

- **Centralizers**: Let $g \in G$, define $\mathbf{C}_G(g) = \{x \in G | xg = gx\}$.

- **Example**: $\mathbf{C}_{D_8}(h) = \{1, h, g^2, g^2h\}$.

- **Lemma 2.12**: $\mathbf{C}_G(x) \leq G$.

- Define center of G as $Z(G) = \bigcap_{n \in G} \mathbf{C}_G(h)$.

- **Example**: $Z(D_8) = \{1, g^2\}$.

- $\mathbf{C}_G(x) \leq G$. For a set Y, $\mathbf{C}_G(Y) = \bigcap_{x \in Y} \mathbf{C}_G(x) \leq G$. $Z(G) = \mathbf{C}_G(G) \leq G$.

- **Conjugation**: For $g, h \in G$, we define $g^h = h^{-1}gh$. Then we have $(g^h)^k = (h^{-1}gh)^k = k^{-1}h^{-1}ghk = (hk)^{-1}g(hk) = g^{hk}$.

- **Automorphisms**: An isomorphism from a group to itself is called an automorphism.

- **Example**: For $\{1, g, g^2, g^3\}$, the automorphism ϕ can be defined as $\{1 \to 1, g \to g^3, g^2 \to g^2, g^3 \to g\}$.

- $\mathrm{Aut}(G) =$ set of all automorphism of G, closed under composition, inverses, contains the identity map group!

- Note: $\mathrm{Aut}(G) = \mathrm{Sym}(G)$.

- **Inner Automorphisms**: Let $g \in G$. The map $\theta_g : G \to G$ defined by $\theta_g(x) = x^g$ is an automorphism of G. (If G is abelian, then θ_g would be trivial, say it is identity map.)

- The set of all inner automorphism of G forms a group called $\mathrm{Inn}(G)$. Note: $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Why? $\theta_g\theta_n = \theta_{gn}, \theta_g^{-1} = \theta_{g^{-1}}$.

  Proof. Note that $\mathrm{Inn}(G)$ is nonempty, since $\theta_1 \in \mathrm{Inn}(G)$. Now let $\theta_g, \theta_n \in \mathrm{Inn}(G)$. Then, for $x \in G$, $\theta_g(\theta_h)^{-1}(x) = \theta_h^{-1}(x^g) = x^{gh^{-1}} = \theta_{gh^{-1}}(x)$, since $\theta_h^{-1} = \theta_{h^{-1}}$. Then $\theta_g\theta_h^{-1} \in \mathrm{Inn}(G)$. Therefore, $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

- **Example**: $D_8 = \{1, g, g^2, g^3, h, gh, g^2h, g^3h\}$. $\theta_g = \{1 \to 1, g \to g, g^2 \to g^2, g^3 \to g^3, h \to g^2h, gh \to g^3h, g^2h \to h, g^3h \to gh\}$ is an inner automorphism while $\theta_h = \{1 \to 1, g \to g, g^2 \to g^2, g^3 \to g^3, h \to gh, gh \to g^2h, g^2h \to g^3h, g^3h \to h\}$ is not an inner automorphism.

- **Example**: $S_5 = \mathrm{Sym}(\{1, 2, 3, 4, 5\})$, $\mathrm{Aut}(G) = \mathrm{Inn}(S_5)$.

- Group U_n where $U_n = \{a \in \mathbb{Z} | 0 \leq a < n, \gcd(a, n) = 1\}$ under multiplication modulo n.

- **Example**: $U_5 = \{1, 2, 3, 4\}$, $U_6 = \{1, 5\}$, $U_{10} = \{1, 3, 7, 9\}$, $U_{12} = \{1, 5, 7, 11\}$.

- Let $\mathbb{Z}_{10}$ be arithmetic modulo 10 under addition. What is $\mathrm{Aut}(\mathbb{Z}_{10})$? We can construct automorphisms from U_{10}. For $3 \in 10$, define $\phi : \mathbb{Z}_{10} - \mathbb{Z}_{10}$ via $\phi : x \to 3x$ is an automorphism.

- $\mathrm{Aut}(\mathbb{Z}_{10}) \cong U_n$. Since the generators of $U_n = \{1, 3, 7, 9\}$ are in $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

- **Example**: $D_8 = \{1, g, g^2, g^3, h, gh, g^2h, g^3h\}$, $H = \langle g \rangle$ - preserved by all automorphisms of D_8 (as a subgroup). $K = \{1, h\}$, $\theta_g(K) = \{1, g^2h\} \neq K$.

- **Characteristic**: We $H \leq G$ is characteristic in G provided that $\sigma(h) \in \mathrm{Aut}(G)$.

- **Theorem**: $Z(G)$ char G.

  Proof. Let $\phi \in \text{Aut}(G)$. Let $h \in Z(G)$. We first show $\phi(h) \in Z(G)$. Let $w \in G$. Since ϕ is a bijection for some $x \in G$. Then $w\phi(h) = \phi(x)\phi(h) = \phi(xh) = \phi(hx) = \phi(h)\phi(x) = \phi(h)x$. Therefore, $\phi(h) \in Z(G)$ proving $\phi(Z(G)) \leq Z(G)$. Using the same argument on ϕ^{-1}, we also obtain $\phi^{-1}(Z(G)) \leq Z(G)$. Applying ϕ, $Z(G) = \phi^{-1}\phi(Z(G)) \leq \phi(Z(G))$. So $Z(G) = \phi(Z(G))$.

- **Normal subgroup**: We call a subgroup $H \leq G$ normal in G if H is fixed (setwise) by every inner automorphism of G. Equivalently, $H \lhd G$ provided that $H^g = H$ for all $g \in G$.

- Note: characteristic subgroups are also normal.

- **New groups from old**: Given group H, G with operation $\circ$ and $\bigstar$, we define a new group on $H \times G = \{(h, g) | h \in H, g \in G\}$, where the new operation $(h_1, g_1)(h_2, g_2) = (h_1 \circ h_2, g_1 \bigstar g_2)$, the identity is the direct sum of their identities, say $(1_H, 1_G)$.

- **Example**: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ is isomorphic to $\{1, g, g^2, h, g^2h\} \leq D_8$. $\mathbb{Z}_2 \times D_8 = \{(0,1), (0,g), (0,g^2), \ldots, (1,1)$

- Note: In an Abelian group, every subgroup is normal. $\mathbb{Z}_2 \times \mathbb{Z}_2$ has the subgroup $H = \{(0,0), (0,1)\}$, $H \lhd \mathbb{Z}_2 \times \mathbb{Z}_2$

- Is H char $\mathbb{Z}_2 \times \mathbb{Z}_2$? No. Let $\sigma \in \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ where $\sigma(x, y) = (y, x)$, but $\sigma(H) \neq H$.

- **Lemma 2.15**: Let H be a subgroup of G, then $H \lhd G$ if and only if $H^g \leq H$ for all $g \in G$.

  Proof. Let $H \leq G$ and suppose $H^g \leq G$ for all $g \in G$. Then for all $g \in G, H^{g^{-1}} \leq H$. So $(H^{g^{-1}})^g \subseteq H^g$, implying $H \subseteq H^g$ for all $g \in G$. Therefore, $H = H^g$ for all $g \in G$.

- **Corollary**: Let $H \leq G$, then $H \lhd G$ if and only if for each $h \in H$, $g \in G$, we have $h^g \in H$.

- **Example**: In $GL(n, \mathbb{C})$, the subgroup $SL(n, \mathbb{C}) = \{M \in GL(n, \mathbb{C}) \text{ with } \det(M) = 1\}$, $SL(n, \mathbb{C}) \lhd GL(n, \mathbb{C})$. If $M \in SL(n, \mathbb{C})$, $N \in GL(n, \mathbb{C})$, $M^N = N^{-1}MN$. $\det(M^N) = \det(N^{-1}) \det(M) \det(N) = 1$.

- **Normal subgroup** is not transitive. That is, it can happen that $H \lhd K, K \lhd G$, but $H \not\lhd G$.

- Note: $K = \{1, g^2, h, g^2h\} \lhd D_8$, $g^{-1}hg = g^2h$, $H = \{1, h\} \lhd K$ but $H \lhd G$.

- **Lemma 2.16**: Suppose H char N and $N \lhd G$, then $H \lhd G$.

  Proof. Let g be a memeber of G ($g \in G$), consider $\theta_g \in \text{Inn}(G)$ (inner automorphism). Since $\theta_g(N) = N$. $\theta_g|_N$ is an automorphism of N. Since H char N, $(\theta_g|_N)(H) = H$. So $H^g = H$ implying $H \lhd G$.

- **Theorem 2.17** Let G be any group. Then $\text{Inn}(G) \lhd \text{Aut}(G)$. Reason: $\theta_g^\sigma = \theta_{\sigma(g)}$, for $\sigma \in \text{Aut}(G)$.

- **Lemma**: Let $X, Y, Z \subseteq G$ and let $H \leq G$. Recall $XY = \{xy : x \in X, y \in Y\}$. Then $(XY)Z = X(YZ)$. Also, $X \subseteq HX$, and $X \subseteq XH$. Lastly, $HH = H$.

  Proof. Note $(XY)Z = \{(xy)z : x \in X, y \in Y, z \in Z\} = \{x(yz) : x \in X, y \in Y, z \in Z\} = X(YZ)$. Next, note that $1 \in H$. Since $H \leq G$, so $X = \{1x : x \in X\} \subseteq hx : h \in H, x \in X = HX$. Similarly, we see $X \subseteq XH$. Lastly, by closure $HH \subseteq H$. However, by the previous fact $H \subseteq HH$. Therefore, $H = HH$.

- **Lemma 2.18**: Let $H, K \subseteq G$, then $HK \subseteq G$ if and only if $HK = KH$.

  Proof. ($\Rightarrow$) Assume $HK \leq G$, we have $H, K \subseteq HK$ (by lemma). Closure implies that $KH \subseteq HK$. Let $x \in HK$. Then $x^{-1} \in HK$, since $HK \leq G$, then $x^{-1} = hk$, for some $h \in H, k \in K$. Then $x = k^{-1}h^{-1} \in KH$. Therefore, $HK \subseteq KH$, forcing $HK = KH$.

  ($\Leftarrow$) Suppose $HK = KH$. Clearly $1 \in HK$, so $HK \neq \emptyset$. Let $x, y \in HK$. Then $x = h_1k_1, y = h_2k_2$ for $h_1, h_2 \in H$, $k_1, k_2 \in K$. This gives $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1(k_1k_2^{-1}h_2^{-1})$. Note $k_1k_2^{-1}h_2^{-1} \in KH = HK$, so $k_1k_2^{-1}h_2^{-1} = h_3k_3$ for some $h_3 \in H$, $k_3 \in K$. Then $xy^{-1} = (h_1h_3)k_3 \in HK$. Therefore, $HK \leq G$.

- **Cosets**: Let $H \leq G$. The right cosets of H are the sets $Hg = H\{g\}$ for $g \in G$. Left cosets: $gH = \{g\}H$ for $g \in G$.

- **Example**: $D_8 = \{1, g, g^2, g^3, gh, g^2h, g^3h\}$.

  - $H = \{1, h\} = Hh$ $- $ $Hg = \{g, g^3h\} = Hg^3h$
  - $Hg^2 = \{g^2, g^2h\} = Hg^2h$
  - $Hg^3 = \{g^3, gh\} = Hgh$

Note: for $h \in H$, $H \leq G$, $Hh = H$. Why? Clearly, $Hh \subseteq H$ by closure. Let $g \in H$. Then $GH^{-1} \in H$, so $gh^{-1}h = g \in Hh$.

- **Lemma 2.20**: Let $H \leq G$.

  (a) If $Hx \cap Hy \neq \emptyset$, then $Hx = Hy$.
  (b) If $xH \cap yH \neq \emptyset$, then $xH = yH$.

  Upshot: right (left) cosets are disjoint or equal.

  Proof. Note $H(hx) = (Hh)x = Hx$ whenever $h \in H$. Suppose $g \in Hx \cap Hy$, then $g = hx = h'y$ for some $h, h' \in H$. So $Hg = Hhx = Hx$ and $Hg = Hh'y = Hy$, which gives $Hx = Hy$.

  Similar proof for left cosets.

- **Lemma 2.22**: Let $H \leq G$. Then all cosets of H have cardinality $|H|$. Why? Map $H \to Hg$ given by $h \mapsto hg$ is a bijection.

- **Definition**: Index of H in G is the number of right (left) cosets of H. Denote: $|G : H|$.

- **Theorem 2.23 (Lagrange)**: Let $H \leq G$. Then $|G| = |H||G : H|$. In particular, if G is finite, $|H|$ divides $|G|$.

  Proof. If $|G|$ is finite, we have G is partitioned into $|G : H|$ right cosets, all of order $|H|$. So $|G| = |H||G : H|$.

- **Corollary 2.24**: Let G be finite, $g \in G$. Then, $\sigma(g)$ divides $|G|$. Also, $g^{|G|} = 1$.

  Proof. We have $\langle g \rangle \leq G$. So $|\langle g \rangle|$ divides $|G|$. Since $|\langle g \rangle| = \sigma(g)$. So $\sigma(g)$ divides $|G|$. Then $g^{|G|} = 1$ follows 2.8(a).

- **Fermat's Little Theorem**: If p is prime, $p \nmid a$, then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

- **Example**: By Fermat's Little Theorem, we know that $183^{16} (\mathrm{mod}\, 17) = 1$, then we can conclude that $183^{33} (\mathrm{mod}\, 17) = 183^{16} \cdot 183^{16} \cdot 183^{1} (\mathrm{mod}\, 17) = 183 (\mathrm{mod}\, 17) = 13$.

- Recall for $g \in G$, $\sigma(g) || G|$ and $g^{|G|} = 1$. Consider $U_n = \{a \in \mathbb{Z} | 0 \leq a \leq n \text{ and } \gcd(a, n) = 1\}$, and known that $|U_n| = \phi(n)$. Note: U_n forms a group under multiplication modulo n. Say $U_8 = \{1, 3, 5, 7\}$ and $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ since $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$.

- **Euler's theorem**: If $\gcd(a, n) = 1$, then $a^{\phi(n)} = 1 (\mathrm{mod}\, n)$.

  Proof. U_n is a group, so $a^{|U_n|} \equiv 1 (\mathrm{mod}\, n)$.

- **Example**: $183^{13} (\mathrm{mod}\, 15) = (183^8)^4 183 (\mathrm{mod}\, 15) = 183 (\mathrm{mod}\, 15) = 3$.

- Recall that normal subgroup $H^g = H$ for $g \in G$ suffices to show $H^g \subseteq H$ for all $g \in G$.

- **Theorem 2.25**: Let $H \leq G$, the following are equivalent (TFAE):

  (1) $H \lhd G$.
  (2) $Hg = gH$.
  (3) Every left cosets is a right cosets.
  (4) Set of right cosets is closed under set multiplication.

  Proof.

  (1) $\Rightarrow$ (2): Let $g \in G$, then $H^g = H$, so $g^{-1}Hg = H$. Multiply by g on left, $Hg = gH$.
  (2) $\Rightarrow$ (3): Clear.
  (3) $\Rightarrow$ (4): Let Hx, Hy be the right cosets of H. The left coset xH must be a right coset Hz, for some $z \in G$ by (3). Then $(Hx)(Hy) = (HxH)g = H(Hz)y = (HH)(zy) = Hzy$.
  (4) $\Rightarrow$ (1): Let $g \in G$. Then Hg^{-1}, Hg are right cosets of H, so $Hg^{-1}Hg = Hz$ for some $z \in G$. Note that $1 \in Hg^{-1}Hg = Hz$ where $Hg^{-1}Hg = \{h_1 g^{-1} h_2 g : h_1, h_2 \in H\}$, so $Hz = H$. Considering $H(g^{-1}Hg) = H$, so $g^{-1}Hg \subseteq H$ since $X \subseteq HX$. Since $H^g = g^{-1}Hg \subseteq H$ for all $g \in G$, $H \lhd G$.

- **Examples**:

  (1) D_8 and let $H = \{1, h\}$. We have $H = \{1, h\}, Hg = \{g, g^3 h\}, Hg^2 = \{g^2, g^2 h\}, Hg^3 = \{g^3, gh\}, gH = \{g, gh\}, g^2 H = \{g^2, g^2 h\}, g^3 H = \{g^3, g^3 h\}$.

(2) Let $H = \{1, g^2\}$. Then $H = \{1, g^2\}, Hg = \{g, g^3\}, Hh = \{h, g^2h\}, Hgh = \{gh, g^3h\}, HgHh = \{gh, g^3h\} = Hgh$.
(3) Let $K = \{1, g, g^2, g^3\}, hK = \{h, g^3h, g^2h, gh\}, Kh = \{h, gh, g^2h, g^3h\}$.

- **Corollary 2.26**: Swap words "left" to "right" in Theorem 2.25.
- **Quotient group**: Let $H \lhd G$, we define $G/H = \{Hg : g \in G\}$with operation of set multiplication.
- **Theorem 2.27**: If $H \lhd G$, G/H is a group with identity. H and with $(Hg)^{-1} = Hg^{-1}$ and multiplication $HxHy = Hxy$.

  Proof. We have closure by theorem 2.25, associativity by our lemma ($(XY)Z = X(YZ)$). So set multiplication is an associative binary operation on G/H. By theorem 2.25 $HxHy = xHHy = xHy = Hxy$. Also, $HHx = Hx$ and $HxH = HHx = Hx$, so H is the identity. Lastly, for any coset Hx, Hx^{-1} is a coset, and $HxHx^{-1} = H \cdot 1 = H$. So $(Hx)^{-1} = Hx^{-1}$.
- **Theorem 2.28**: Let $N \lhd G$, $H \leq G$. Then $NH = HN$, and so $HN \leq G$. Futhermore, if $H \lhd G$, then $HN \lhd G$.

  Proof. We have $HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$. By the previous result (theorem 2.18), $HN \leq G$. Now suppose $H \lhd G$ as well. Then for $g \in G$, $(HN)^g = H^g N^g = HN$.
- **Normalizers**: $\mathbf{N}_G(X) = \{g \in G | X^g = X\}$ where $X \subseteq G$.
- **Lemma 2.29**: We have $\mathbf{N}_G(X) \leq G$. If $X \leq G$, then $X \leq \mathbf{N}_G(X)$.

  Proof. Note $1 \in \mathbf{N}_G(X)$, so $\mathbf{N}_G(X) \neq \emptyset$. Let $g, h \in \mathbf{N}_G(X)$. Then $X^{gh^{-1}} = (X^g)^{h^{-1}} = X^{h^{-1}} = (X^h)^{h^{-1}} = X^{hh^{-1}} = X$. Lastly, if $X \leq G$, then $X^g = X$ for any $g \in X$ by closure. So $X \leq \mathbf{N}_G(X)$.
- **Corollary 2.30**: Let $H \leq G$. Then $H \lhd \mathbf{N}_G(H)$ and for any $K \leq G$ with $H \leq K$, we have $H \lhd K$ if and only if $K \leq \mathbf{N}_G(H)$.
- **Corollary 2.31**: Let $H, K \leq G$. If $K \leq \mathbf{N}_G(H)$, then $HK = KH$, so $HK \leq G$.

  Proof. $KH = \bigcup_{k \in K} kH = \bigcup_{k \in K} Hk = HK$.
- **Example**: $D_8 = \{1, g, g^2, g^3, h, gh, g^2h, g^3h\}$. $\mathbf{N}_{D_8}(\{g^3, gh\}) = \{1, g^2\}$. $\mathbf{N}_{D_8}(\{g\}) = \{1, g, g^2, g^3\}$.
- **Group Theory Software**:
  - GAP (by Alexander Hulpke, free)
  - Magma (free in US for 2 years)
  - Sage
- Shorthand for $\mathrm{Sym}(\{1, \ldots, n\})$ is S_n.
- Take a tetrahedron for example. We get as reflections: $(12), (13), (14)$. Notice that $(123) = (12)(13)$, $(23) = (12)(13)(12)$. $S_4 = \langle (12), (13), (14) \rangle$.
- Denote $K = \{e, (12)(34), (13)(24), (14)(23)\}$, K forms a subgroup of S_4. Called *Klein-4 group*.
- Compute $\mathbf{N}_{S_4}(K)$, $K \leq \mathbf{N}_{S_4}(K)$. $K^{(12)} = \{e, (12)(34), (14)(23), (14)(23)\}$, since $(12)[(12)(34)](12) = (12)(34)$. And same for $K^{(13)} = K, K^{(14)} = K$, so $(12), (13), (14) \in \mathbf{N}_{S_4(K)}$. Henceforth, $\mathbf{N}_{S_4}(K)$, so $K \lhd S_4$.
- **Example**: $H = \langle (1234) \rangle$, denote $N = \mathbf{N}_{S_4}(H)$, $4 || N|$. Since $(1234)^{(24)} = (24)(1234)(24) = (1432)$, etc., we have $H^{(24)} = \{e, (1432), \ldots\} = \langle (1432) \rangle = H$. Note that $H^{(24)}$ is also a cyclic group of order 4 and $H \cong H^{(24)}$. This show $(24) \in N$ as well, so $|N| > 4$. So $|N| = 8, 12, 24$. We claim $\langle H \cup \{(24)\} \rangle$ has order of 4. Note $\langle H \cup \{(24)\} \rangle = \langle (1234), (24) \rangle$ and H is a subgroup. Let's find $|\langle H \cup \{(24)\} : H|$. Cosets: H, $H(24)$. What is $H(24)(1234)$? I claim $(24) \in H(24)(12)$. Note that $H \lhd \langle H \cup \{(24)\} \rangle$ since $\langle H \cup \{(24)\} \rangle \leq N$. $H(24)(1234) = (24)H(1234) = (24)H = H(24)$. So H, $H(24)$ are the only cosets of H in $\langle (24), (1234) \rangle$, so $|\langle (24), (1234) \rangle| = 8$. Lastly, let's consider $H^{(123)} = (132)(1234)(123) = (1423)$, so $|N| =\neq 24$, hence $|N| = 8$, and $N = \langle (24), (1234), \ldots \rangle$.

2 Chapter 3

2.1 Group homomorphism

- A map $\phi : G \to H$ is called homomorphism if $\phi(a, b) = \phi(a)\phi(b)$.
- **Example**: note that $\mathbb{C}^* = \{x \in \mathbb{C} | x \neq 0\}$ is a group under multiplication.
- **Example**: $\phi : GL(n, \mathbb{C}) \to \mathbb{C}^*$ define by $\phi(M) = \det(M)$.
- **Kernel of a homorphism**: $\ker \phi = \{x \in G | \phi(x) = 1\}$.
- **Example**: For ϕ given on $GL(n, \mathbb{C})$, $\ker \phi = SL(n, \mathbb{C})$.
- **Example**: $\phi : G \to \text{Inn}(G)$, $\phi(g) = \theta_g$, $\ker \phi = Z(G)$, since $\theta_g(x) = x$, we have $x^g = g^{-1}xg = x \Rightarrow xg = gx$.
- **Example**: $\phi : \mathbb{Z} \to \mathbb{Z}_n$. $\phi(x) = x (\text{mod } n)$, then $\ker \phi = n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$: $n\mathbb{Z}, n\mathbb{Z} + 1, n\mathbb{Z} + 2, \ldots, n\mathbb{Z} + (n - 1)$.
- **Theorem**: Let $\phi : G \to H$ be a homomorphism, then

  (a) $\phi(1) = 1$, $\phi(x)^{-1} = \phi(x^{-1})$.
  (b) $\ker \phi \lhd G$.
  (c) $\phi(x) = \phi(y)$ if and only if $\mathbf{N}_x = \mathbf{N}_y$ ($x = ny$ for some $n \in N$), where $N = \ker \phi$.
  (d) ϕ is injective if and only if $\ker \phi = \{1\}$.

  Proof.

  (a) We have $\phi(1) \cdot 1 = \phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1)$, then $\phi(1) \cdot 1 = \phi(1) \cdot \phi(1)$. Multiplying by $\phi(1)^{-1}$ we get $\phi(1)^{-1}\phi(1) \cdot 1 = \phi(1)^{-1}\phi(1)\phi(1)$, so $\phi(1) = 1$. Also, $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1) = 1$, so by uniqueness of inverses $\phi(x^{-1}) = \phi(x^{-1})$.
  (b) Let $x \in N, g \in G$, then $\phi(x^g) = \phi(g^{-1}xg) = \phi(g^{-1})\phi(x)\phi(g) = \phi(g^{-1})\phi(g) = 1$. So $x^g \in N$, so $N \lhd G$.
  (c) Suppose $\phi(x) = \phi(y)$, then $\phi(xy^{-1}) = 1$. So $xy^{-1} \in N$. Then $xy^{-1} = n$ for some $n \in N$. So $x = ny$.Then $Nx = Nny = Ny$. Conversely, suppose $Nx = Ny$. Then $y = nx$, for some $n \in N$. Then $\phi(y) = \phi(nx) = \phi(n)\phi(x) = \phi(x)$.
  (d) If $N \neq \{1\}$, then $|N| \geq 2$, so clearly ϕ is not injective. Suppose $N = \{1\}$, let $x, y \in G$ with $\phi(x) = \phi(y)$. Then $\phi(xy^{-1}) = 1$, so $xy^{-1} \in N$. So $xy^{-1} = 1$ implying $x = y$.

- **Corollary 3.2**: The normal subgroups of G are precisely the kernel of homomorphism from G to other groups.

  Proof. From 3.1, kernels are normal. Let $N \lhd G$. Define $\phi : G \to G/N$ via $\phi(x) = Nx$. (Called canonical homomorphism). This is a homomorphism. Since $\phi(xy) = Nxy = NxNy = \phi(x)\phi(y)$. We have $(Ker)\phi = \{x \in G | Nx = N\} = N$.

- **Theorem 3.3 (First Isomorphism Theorem)**: Let $\phi : G \to H$ be a surjective homomorphism. Then $H \cong G/\ker \phi$. Furthermore, there is a unique isomorphism $\theta : G/\ker \phi \to H$ such that $\pi\theta = \phi$, where $\pi : G \to G/\ker \phi$ is the canonical homomorphism.

  Proof. Let $\phi : G \to H$ be surjective homomorphism. Let $\pi : G \to G/N$ be the canonical homomorphism, $N = \ker \phi$. If $\pi\theta = \phi$, we must have $\theta(\pi(x)) = \phi(x)$, so $\theta(Nx) = \phi(x)$. We claim $\theta : G/N \to H$ defined by $\theta(Nx) = \phi(x)$ is an isomorphism. We first show θ is well defined. Suppose $Nx = Ny$. Then $\phi(x) = \phi(y)$ by 3.1 (c). To show it's a homomorphism, note that for $Nx, Ny \in G/N$, $\theta(NxNy) = \theta(Nxy) = \phi(xy) = \phi(x)\phi(y) = \theta(Nx)\theta(Ny)$. The map θ is surjective because ϕ is surjective. Lastly, the kernel of θ, $\ker \theta = \{Nx : \phi(x) = 1\} = \{Nx : x \in N\} = \{N\}$. So θ is injective. Therefore, θ is an isomorphism and $G/N \cong N$.

- **Example**: $GL(n, \mathbb{C})/SL(n, \mathbb{C})$. Define $\phi : GL(n, \mathbb{C}) \to \mathbb{C}^*$ via $\phi(M) = \det(M)$. $\ker \phi = SL(n, \mathbb{C})$. Note: ϕ is surjective so $GL(n, \mathbb{C})/SL(n, \mathbb{C}) \cong \mathbb{C}^*$.
- **Corollary**: Let $\phi : G \to H$ be a homomorphism, then $G/\ker \phi \cong$ image of H.
- For $U \subseteq G$, $V \subseteq H$, $\phi : G \to H$, $\phi(U) = \{\phi(x) : x \in U\}$. $\phi^{-1}(V) = \{x \in G | \phi(x) \in V\}$, $\phi^{-1}(\{1\}) = \ker \phi$.
- **Lemma 3.5**: Let $\phi : G \to H$ be a homomorphism.

  (a) If $U \leq G$, then $\phi(U) \leq H$.

(b) If $V \leq H$, $\phi^V \leq G$ with $\ker\phi \leq \phi^{-1}(V)$.

Proof.

(a) Since $U \neq \emptyset$, $\phi \neq \emptyset$. Let $\phi(x), \phi(y) \in \phi(U)$. Then $\phi(x)\phi(y)^{-1} = \phi(xy^{-1}) \in \phi(U)$ since $xy^{-1} \in U$. So $\phi(u) \leq H$.
(b) Note the identity $1 \in \phi^{-1}(V)$, so $\phi^{-1}(V) \neq \emptyset$. Let $x, y \in \phi^{-1}(V)$. Then, $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in V$, since $\phi(x), \phi(y) \in V$. So $xy^{-1} \in \phi^{-1}(V)$. So $\phi^{-1}(V) \leq G$. Lastly, since $\phi(\ker\phi) = \{1\} \subseteq V$, we have $\ker\phi \subseteq \phi^{-1}(V)$.

- **Theorem 3.6**: Let $N \lhd G$, $H \leq G$. Then $H \cap N \lhd H$ and $H/H \cap N \cong NH/N$.

  Proof. Let $\pi : G \to G/N$ be the canonical homomorphism. Let $\phi = \pi|_H$. Note that now ϕ is a homomorphism from H to G/N. Note that $\text{img}(\phi) = \{Nx : x \in H\} = \{Nyx : y \in N, x \in H\} = \{Nz : z \in NH\} = NH/N$. So $H/\ker\phi \cong \text{im}(\phi) = NH/N$. Lastly, we compute $\ker\phi = \{x \in H : Nx = N\} = H \cap N$. So $H/H \cap N \cong NH/N$.

- **Theorem 3.7 (Correspondence theorem)**: Let $\phi : G \to H$ be a surjective homomorphism, $N = \ker\phi$. Let $S = \{U | N \leq U \leq G\}$, $T = \{V | V \leq H\}$. Then ϕ, ϕ^{-1} defines inverse bijection between S and T. Furthermore, that maps repsect containment, indices, normality, and factor groups. In other words, $\phi(U_1) = V_1$, $\phi(U_2) = V$.

  - $U_1 \leq U_2 \Leftrightarrow V_1 \leq V_2$.
  - $|U_2 : U_1| = |V_2 : V_1|$.
  - $U_1 \lhd U_2$ iff $V_1 \lhd V_2$.
  - $U_2/U_1 \cong V_2/V_1$.

  Proof. By 3.5, ϕ, ϕ^{-1} are maps between S and T. We will show they are inverses of each other. Let $U \in S$. Clearly, $U \subseteq \phi^{-1}(\phi(U))$. Let $g \in \phi^{-1}(\phi(U))$. Then $\phi(g) \in \phi(U)$. So $Ng = Nu$ for some $u \in U$ ($\phi(g) = \phi(u)$ for some $u \in U$). Therefore, $g \in Ng = Nu \subseteq U$. Since $u \in U, N \subseteq U$. Therefore, $\phi^{-1}(\phi(U)) = U$. Let $V \in T$. Clearly, $\phi(\phi^{-1}(V)) \subseteq V$. Let $v \in V$. Since ϕ is surjective, $\exists g \in G$ with $\phi(g) = v$. Then, $g \in \phi^{-1}(V)$, so $v = \phi(g) \in \phi(\phi^{-1}(V))$. So $\phi(\phi^{-1}(V)) = V$. Therefore, ϕ, ϕ^{-1} are inverse bijections form S to T. Clearly, ϕ, ϕ^{-1} respect containment. Let $U_1 \lhd U_2 \leq G$. Let $z \in \phi(U_2)$, then $z = \phi(x)$ for some $x \in U_2$ (surjectivity), so $\phi(U_1)\phi(x) = \phi(U_1^x) = \phi(U_1)$, so $\phi(U_1) \lhd \phi(U_2)$.

- $S = \{U \leq G, \ker\phi \subseteq U\}$, $\phi : G \to H$ surjective, $T = \{V \leq H\}$, ϕ, ϕ^{-1}.

- Suppose $U_1, U_2 \in S$, $U_1 \leq U_2$, $\phi(U_1) \lhd \phi(U_2)$. Let $x \in U_2$. Then $\phi(U_1^x) = \phi(U_1)^{\phi(x)} = \phi(U_1)$, since $\phi(x) \in \phi(U_2)$. Since $\phi(U_1^x) = \phi(U_1)$, and $U_1^x, U_1 \in S$, and ϕ is a bijection from S to T, we must have $U_1^x = U_1$. Therefore, $U_1 \lhd U_2$.

- Let $U_1 \lhd U_2$, $V_1V_2 = \phi(U_1)\phi(U_2)$ respectively. Note $V_1 \lhd V_2$.

- Let $\pi : V_2 \to V_2/V_1$ be the canonical homomorphism, let ϕ' be the restriction of ϕ to U_2. Let $\theta = \phi'\pi$. So $\theta : U_2 \to V_2/V_1$. Note $\theta(U_2) = \pi(\phi'(U_2)) = \pi(\phi(U_2)) = \pi(V_2) = V_2/V_1$, so θ is surjective. Lastly, $\ker\theta = \{x \in U_2 | \pi(\phi'(x)) = V_1\} = \{x \in U_2 | V_1\phi'(x) = V_1\} = \{x \in U_2 | \phi'(x) \in V_1\} = U_1$. Therefore, $U_2/U_1 \cong V_2/V_1$. Lastly, we show indices are preserved. Let $U_1 \leq U_2$, $U_1, U_2 \in S$, and $V_1 = \phi(U_1), V_2 = \phi(U_2)$. We construct a bijection from $\{U_1x | x \in U_2\}$ to $\{V_1y | y \in V_2\}$. We use $\phi(U_1x) = V_1\phi(x)$. We first show this map is surjective. Let $z \in V_2$, so V_1z is a coset of V_1. Then $z = \phi(x)$ for some X in U_2, so $\phi(U_1x) = V_1z$. To show it's injective, suppose $\phi(U_1x) = \phi(U_1y)$, where $x, y \in U_2$. Then $V_1\phi(x) = V_1\phi(y)$, so $\phi(x)\phi(y)^{-1} \in V_1$. Then $\phi(xy^{-1}) \in V_1$, so $xy^{-1} \in \phi^{-1}(V_1) = U_1$. So $U_1x = U_2y$. Therefore, the map is bijective, and $|U_2 : U_1| = |V_2 : V_1|$.

- **Corollary 3.8**: Let $N \lhd G$. Every subgroup of G/N has the form H/N for a unieq subgroup $H \leq G$ with $N \leq H$.

  Proof. Let $\pi : G \to G/N$ be the canonical homomorphism. So by the correspondence theorem, subgroups of G/N correspondent to subgroups of G containing $\ker(\phi) = n$. So given $M \leq G/N$, we have a unique subgroup H with $N \leq H$, $\phi(H) = M$ and $H/N \cong M/\{1\} \cong M$. ($N \leq H \leq G \Rightarrow \pi(N) \leq \pi(H) \leq \pi(G)$) and $\pi(H) = H/N = \{Nx : x \in H\}$.

- **Corollary 3.9**: Let $N \leq M \lhd G$ and $N \lhd G$. Then $(G/N)/(M/N) \cong G/M$.

  Proof. Let $\pi : G \to G/N$ be the canonical homomorphism. We have $M \lhd G$, $N \leq M$, and so $\pi(M) = M/N \lhd \pi(G) = G/N$. By 3.7, $G/M \cong (G/N)/(M/N)$.

- **Exercise**: Show $\text{Inn}(G)$ cannot be nontrivial cyclic group.

- **Definition**: Define $\phi : G \to \text{Inn}(G)$ via $\phi(g) = \theta_g$. We have $\ker(\phi) = Z(G)$. So by the last isomorphism theorem, $G/Z(G) \cong \text{Inn}(G)$. Note: ϕ is clearly surjective. By way of contradiction, suppose $G/Z(G)$ is nontrivial and cyclic. Then $G/Z(G) = \langle Z(G)x \rangle = \{Z(G)x^i, i \in \mathbb{Z}\}$. Therefore, every element of G has the form zx^i where $z \in Z(G), i \in \mathbb{Z}$. This forces G to be abelian, so $Z(G) = G$, so $\text{Inn}(G)$ is trivial cyclic.

- **Definition**: Define the commutator of x and y to be $[x,y] = x^{-1}y^{-1}xy$. Note: x commutes with y if and only if $[x,y] = 1$. Commutator group denoted as $G' = \langle\{[x,y] : x,y \in G\}\rangle$.
- **Example**: $D_8 = \{1, x, x^2, x^3, h, xh, x^2h, x^3h\}$, then $D_8' = \{1, x^2\}$. Note: for a homomorphism, $\phi([x,y]) = [\phi(x), \phi(y)]$. If $\phi : G \to H$ is an isomorphism, then $\phi(G') = H'$. In particular, G' char G, so $G' \lhd G$. Note: G is abelian iff $G' = \{1\}$.
- **Theorem 3.10**: Let $N \lhd G$. Then G/N is abelian iff $G' \subseteq N$.

  Proof. Let $\pi : G \to G/N$ be canonical homomorphism. Suppose G/N is abelian. Then $\pi([x,y]) = [\pi(x), \pi(y)] = 1$. $\pi(G') = \{1\}$. So $G' \leq \ker(\phi) = N$. Conversely, suppose $G' \subseteq N$. Then, $\pi(G') = 1$, so $\pi([x,y]) = 1$ for all $x, y \in G$. Since π is surjective, we have $(G/N)' = \langle\{[\pi(x,y)] : x,y \in Gl\}\rangle = \{1\}$. So G/N is abelian.
- **Corollary 3.11**: Let $\phi : G \to A$ be a homomorphism from G to an abelian group A, then $G' \leq \ker(\phi)$.

  Proof. We have $\text{im}(\phi) \leq A$ is abelian and $\text{im}(\phi) \cong G/\ker(\phi)$, so $G' \leq \ker(\phi)$ by the previous theorem.
- **Corollary 3.12**: Let $G' \leq H \leq G$, then $H \lhd G$.

  Proof. Since G/G' is abelian, $H/G' \lhd G/G'$. By the correspondence theorem, using canonical homomorphism $\phi : G \to G/G'$, then $H \lhd G$.
- **Example**: $\{1, x^2, y, x^2y\} \lhd D_8$.

  Commutator of S_n (symmetric group which has n elements) is A_n (alternating group on n elements)
- **Definition**: A *permutation group* is a subgroup of $\text{Sym}(X)$ for some nonempty set X.
- **Example**: $\{\varepsilon, (1432), (13)(24), (1234), (14)(32), (24), (12)(34), (13)\}$, $D_8 \leq S_4$, $D_{2n} \leq S_n$.
- **Example**: $H = \langle\{(12), (345)\}\rangle \leq S_5 = \{\varepsilon, (12), (345), (354), (12)(345), (12)(354)\}$. $\mathbf{C}_n = \langle(12\cdots n)\rangle$.
- **Definition**: Let G be a permutation group on a set X, $\alpha \in X$. The orbit containing α is the set $\mathcal{O}_\alpha = \{(\alpha)\cdot g : g \in G\}$.
- If a permutation group has only one orbit, we call it transitive. That is, for each $\alpha, \beta \in X$, $\exists g \in G$ with $(\alpha)\cdot g = \beta$.
- **Definition**: $S = \text{Stab}_{D_8}(1) = \{\varepsilon, (24)\}$, its cosets are
  - $S = \{1, xy\}$
  - $S_x = \{x, y\}$
  - $S_{x^2} = \{x^2, x^3y\}$
  - $S_{x^3} = \{x^3, x^2y\}$
- **Definition**: One definition of a group G acting on a set X is a homomorphism $\phi : G \to \text{Sym}(X)$.
- **Example**: $D_8 = \{1, x, x^2, x^3, h, xh, x^2h, x^3h\}$, let d_1, d_2 be the group action on D_8 gives $\{\varepsilon, (12), \varepsilon, (12), (12), \epsilon, (12), \varepsilon\}$, kernel of this group action is $\{1, x^2, xh, x^3h\}$.
- **Definition**: Let G be a group, Ω a set with $\Omega \neq \emptyset$. Suppose for all $\alpha \in \Omega$, $g \in G$, there is an operation defined with $\alpha \cdot g \in \Omega$ (that is, $\cdot$ is a function from $\Omega \cdot G$ to Ω) satisfying
  (a) $\alpha \cdot 1 = \alpha$ for all $\alpha \in \Omega$.
  (b) $(\alpha \cdot g) \cdot h = \alpha \cdot (gh)$ for $g, h \in G, \alpha \in \Omega$.
- *Right regular action* of G on itself: $\forall x \in G, g \in G$, we have $x \cdot g = xg$.
- *Conjugation action* of G on itself: $\forall x, g \in G$, we have $x \cdot g = x^g$.
- Action on cosets of $H \leq G$ for a coset $Hx \in G, g \in G$, we have $Hx \cdot g = Hxg$.
- **Kernel of a group action**: $\{g \in G | \alpha \cdot g = \alpha, \forall \alpha \in \Omega\}$.
- Let G be a group, Ω a set. A homomorphism $\phi : G \to \text{Sym}(\Omega)$ defines a group action via $\alpha \cdot g = (\alpha)\phi(g)$.

- **Lemma 4.2**: Let G act on Ω. For $g \in G$, define $\pi g : \Omega \to \Omega$ with $(\alpha)\pi g = \alpha \cdot g$. Then $\pi g \in \mathrm{Sym}(\Omega)$ and $\theta : G \to \mathrm{Sym}(\Omega)$ via $\theta(g) = \pi_g$ is a homomorphism whose kernel is the kernel of the action.

  Proof. We have $(\alpha)(\pi_g \pi_h) = (\alpha \cdot g)\pi h = (\alpha \cdot g) \cdot h = \alpha \cdot (gh) = (\alpha)\pi_{gh}$. So $\pi_g \pi_h = \pi_{gh}$. Also $(\alpha)\pi_1 = \alpha \cdot 1 = \alpha$ for all α. So π_1 is the identity. Similarly, $\pi_{g^{-1}}\pi_g = \pi_1$. So π_g has left and right inverse, imply it is a bijection (permutation). So $\pi g \in \mathrm{Sym}(\Omega)$. Lastly, $\theta(gh) = \pi_{gh} = \pi_g \pi_h = \theta(g)\theta(h)$ so θ is a homomorphism.

- **Corollary 4.3**: Let G act on Ω, N be the kernel of this action. Then, $N \lhd G$ and G/N is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$.

  Proof. Let θ, π_g be as given in previous proof. Then $\theta : G \to Sym(\Omega)$ with kernel N. Therefore, $\mathrm{im}(\theta) \cong G/N$, where $\mathrm{im}(G) \leq \mathrm{Sym}(\Omega)$.

- A group action is called "faithful" if the kernel is $\{1\}$.

- **Definition**: Define a group G is simple if the only normal subgroup of G are $\{1\}, G$.

- Procedures: Take G, and maximal normal subgroup N. Compare G/N, this is simple. Take a maximal normal subgroup $\mathbf{N}_2$ of $\mathbf{N}_1$. Get $\mathbf{N}_1/\mathbf{N}_2$ simple, keep repeating, $G/\mathbf{N}_1, \mathbf{N}_1/\mathbf{N}_2, \mathbf{N}_2/\mathbf{N}_3, \ldots$, which is called composition factors.

- **Classification theorem of finite simple groups**: over 100 authors and over 1000 pages. Answer: there are three infinite families:

  (1) $A_n, n \geq 5$;
  (2) $\mathbb{Z}_p$, p is prime;
  (3) Group of Lie type (matrix groups);
  (4) 26 sporadic examples (monster). (using software called "Cog").

- **Theorem 4.4**: Let $H \leq G$, $|G : H| = n \leq \infty$. Then there is normal subgroup N in G with

  (a) $N \leq H$.
  (b) $|G : N| \big| n!$. In particular, if $n > 1$, $|G| \nmid n!$, then G is not simple.

  Proof. Let G act on the cosets of H. Let N be the kernel of this action. Note: $N \leq H$. Then, there is a homomorphism from G to $S = \mathrm{Sym}(\{Hx : x \in G\})$ with kernel N, and G/N is isomorphic to a subgroup of G. Since the order of a subgroup divides the order of the group, $|G/N|$ divides $|S|$. So $|G : N| \big| n!$ (where $n = |G : H|$). If $n > 1$ and G is simple, we must have $N = \{1\}$, so $|G| \big| n!$.

- **Example**: Let G be a group of order 100 with a subgroup H of order 25. Can G be simple?

  No. $|G : H| = 4$, but $G \nmid 4!$.

- **Example**: $D_8 = \{1, x, x^2, x^3, h, xh, x^2h, x^3h\}$, define $\{(D_8)_1 = g \in D_8 : (1) \cdot g = 1\}$, called the stabilizer of 1 in D_8. For $H = (D_8)_1 = \{\varepsilon, xh\}$

  - $H = \{\varepsilon, xh\}$;
  - $Hx = \{x, h\}$;
  - $Hx^2 = \{x^2, x^3h\}$;
  - $Hx^3 = \{x^3, x^2h\}$.

- **Corollary 4.5**: Let $H \leq G$, G finite and $|G : H| = p$ where p is the smallest prime divisor of $|G|$, then $H \lhd G$.

  Proof. Let G act on the cosets of H. If $|G| \big| p!$, $|G| = p$, so $H = \{1\} \lhd G$. If $|G| \nmid p!$, then the kernel N of this action is a nontrivial ($N \neq \{1\}$) subgroup of H. Let $|H : N| = m$. Then $|G : N| = |G : H||H : N| = pm$. So $pm | p!$, giving $m | (p-1)!$. This forces $m = 1$ by the minimality of the prime divisor p. Therefore, $H = N \lhd G$.

- **Theorem 4.7**: Let $H \leq G$, N the kernel of the action of G on right cosets of H. Then

  (a) $N = \bigcap_{x \in G} H^x$.
  (b) If $M \lhd G$ and $M \leq H$, then $M \leq H$.

  Proof.

(a) Let N, G, H be as given, we have $g \in N$ if and only if $Hx = Hxg$ for all $x \in G$ iff $x^{-1}Hx = x^{-1}Hxg \forall x \in G$ iff $H^x = H^x g \forall x \in G$ iff $g \in H^x \forall x \in G$ iff $g \in \bigcap_{x\in G} H^x$.
(b) Suppose $M \leq H$, $M \lhd G$. Then $M = \bigcap_{x\in G} M^x \subseteq \bigcap_{x\in G} H^x = N$.

- **Definition**: $\mathrm{Core}_G(H) = \bigcap_{x\in G} H^x$ the largest normal subgroup of G contained in H.
- **Definition**: Let G action on Ω, $\alpha \in \Omega$, then the stabilizer is $\mathrm{Stab}_G(\alpha) = G_\alpha = \{g \in G | (\alpha) \cdot g = \alpha\}$.
- **Example**: Let $G = S_5$, $G_5 \cong S_4$.
  - For G acting on cosets of H, $G_H = H$.
  - For G acting on the power set of G, Ω, by conjugation. By convention, $\Phi^g = \Phi, \forall g \in G$. For $x \in \Omega, X^g = \{h^g | h \in X\}$.

  Suppose we have $h \in G$, $G_h = G_{\{h\}} = \mathbf{C}_G(h)$. For $X \subseteq G$, $G_x = \mathbf{N}_G(X)$. If you want the set of elements of G that fix each element of X, then $\mathbf{C}_G(X)$ is pointwise stabilizer of X.
- **Definition**: For $\alpha \in \Omega$, we define $\mathcal{O}_\alpha = \{\alpha^g | g \in G\}$, called the orbit containing α.
- Suppose $\beta \in \mathcal{O}_\alpha$. What is the relationship between $\mathcal{O}_\alpha$ and $\mathcal{O}_\beta$? They are same.
- **Lemma 4.8**: The orbits of G acting on Ω partition Ω.

  Proof (Sketch): Define a relation $\alpha \sim \beta$ if $\beta \in \mathcal{O}_\alpha$. This is an equivalent relation.
- **Theorem 4.9**: Let G act on Ω with $\mathcal{O}$ an orbit. Let $\alpha \in \mathcal{O}$ and $H = G\alpha$. Then there is a bijection between $\mathcal{O}$ and the cosets of H.

  Proof. Let $f : \mathcal{O} \to \{Hx | x \in G\}$ be defined as follows. For $\beta \in \mathcal{O}$, we have $f(\beta) = Hx$ provided that $\alpha \cdot x = \beta$. We need to show f is well-defined. Suppose $f(\beta) = Hx, f(\beta) = Hy$. Then $\alpha \cdot x = \beta = \alpha \cdot y$. So $\alpha \cdot (xy^{-1}) = \alpha$ implying $xy^{-1} \in H$. Therefore, $Hx = Hy$. So f is well-defined. It is clear f is surjective, since $\alpha \cdot x \in \mathcal{O}$ for any $x \in G$, and $f(\alpha \cdot x) = Hx$. Lastly, suppose $f(\beta) = f(\gamma)$ for $\beta, \gamma \in \mathcal{O}$. Then $\beta = \alpha \cdot x, \gamma = \alpha \cdot y$ for some $x, y \in G$. Then $f(\beta) = f(\gamma)$ implies $Hx = Hy$, so $xy^{-1} \in H$. We have $\alpha = \alpha(xy^{-1})$ so $\alpha \cdot y = \alpha \cdot x$, giving $\beta = \gamma$. Therefore f is a bijection from $\mathcal{O}$ to the cosets of H.
- **Theorem 4.10 (Fundamental Counting Principle)**: $|\mathcal{O}| = |G : G_\alpha|$ where $\mathcal{O}$ is an orbit of G acting on Ω, $\alpha \in \mathcal{O}$. If G is finite, $|\mathcal{O}| = |G|/|G_\alpha|$. In particular, $|\mathcal{O}||G|$.
- **Example**: Stabilizer of vertex 4 is in S_4. Let $H = \{\varepsilon, (123), (132)\}$. Then the corresponding cosets are $H(1234), H(13)(24), H(14$
- **Corollary 4.10**: Let G act on Ω, where G is finite, $\mathcal{O}$ be an orbit, $\alpha \in \mathcal{O}$. Then $|\mathcal{O}| = |G|/|G_\alpha|$.
- **Definition**: The conjugacy class containing $g \in G$ is $\mathrm{cl}(g) = \{g^h : h \in G\}$.
- **Example**: $D_8 = \{1, x, x^2, x^3, h, xh, x^2h, x^3h\}$. $\mathrm{cl}(D_8) : \{\varepsilon\}, \{x, x^3\}, \{x^2\}, \{h, x^2h\}, \{xh, x^3h\}$. Note: with G acting on itself by conjugation $\mathcal{O}_g = \mathrm{cl}(g)$. The size of conjugacy class $|\mathrm{cl}(g)| = |G|/|\mathbf{C}_G(g)|$. $\mathbf{N}_G(g) = \mathbf{C}_G(g) \Rightarrow g^h = g$.
- **Corollary 4.11**: we have $|\mathrm{cl}(g)| = |G : \mathbf{C}_G(g)|$.
- **Example**: $|G| = n < \infty$, $1, n-1 \Rightarrow n = 2$.
- **Corollary 4.17**: Let $H, K \leq G$, where H, K are finite: $|HK| = \frac{|H||K|}{|H\cap K|}$.

  Proof. Let K act on the right cosets of H in G. Let $\mathcal{O}$ be the orbit of this action containing the coset H. We have $|HK| = |\bigcup_{g\in K} Hg| = |H||\mathcal{O}|$.
- **Example**: The group actions are as follows: H, Hx, Hx'. The stabilizer in H in this action is $H \cap K$, so $|\mathcal{O}| = \frac{|K|}{|H\cap K|}$, therefore, $|HK| = \frac{|H||K|}{|H\cap K|}$.
- **Definition**: The permutation character of a group action is the map $\chi : G \to \mathbb{C}(\mathbb{N} \cup \{0\})$ be defined by $\chi(g) = |\{\alpha \in \Omega : \alpha \cdot g = \alpha\}|$.

- **Theorem 4.18 (Cauchy-Frobenius theorem)**: Let G act on Ω, where G, Ω are finite. Let n be the number of orbits of this action satisfies: $n = \frac{1}{|G|}\sum_{g\in G}\chi(g) =$ average value of the permutation character.

  Proof. Let G act on Ω, both G and Ω are finite. Let $S = \{(\alpha, g) : \alpha \in \Omega, g \in G, \alpha \cdot g = \alpha\}$. We have $|S| = \sum_{\alpha\in\Omega}$ and $|S| = \sum_{g\in G}\chi(g)$. So $\sum_{g\in G} = \chi(g) = \sum_{\alpha\in\Omega}|G_\alpha|$. This gives

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{\alpha\in\Omega}|G_\alpha| = \sum_{\alpha\in\Omega}\frac{|G_\alpha|}{|G|} = \sum_{\alpha\in\Omega}\frac{1}{|\mathcal{O}_\alpha|} = \sum_{\text{distinct orbits } \mathcal{O}}\sum_{\alpha\in\mathcal{O}}\frac{1}{\mathcal{O}} = \sum_{\text{distinct orbits } \mathcal{O}} 1 = \text{ number of orbits.}$$

- **Example**: a merchant makes 10 necklaces with 10 beads each, chosen from 5 different colors. How many different necklaces are possible?
- **Definition**: An "ordered necklace" is a circular arrangement of 10 beads (where order of beads matters) where there is a clearly labeled first bead, second bead, ..., etc. and labels increase clockwise. Consider different if beads in position i are different for some i.
- **Solution**: We calculate the character of the dihedral group.

g	$\chi(g)$	g	$\chi(g)$
e	5^{10}	h	5^5
x	5	xh	5^6
x^2	5^2	x^2h	5^5
x^3	5	x^3h	5^6
x^4	5^2	x^4h	5^5
x^5	5^5	x^5h	5^6
x^6	5^2	x^6h	5^5
x^7	5	x^7h	5^6
x^8	5^2	x^8h	5^5
x^9	5	x^9h	5^6

  Then, by Cauchy-Frobenius theorem, we have

$$\frac{1}{20}\left(5^{10} + 4\cdot 5 + 4\cdot 5^2 + 5^5 + 5\cdot 5^5 + 5\cdot 5^6\right).$$

- **Theorem 4.19**: Let G be a finite group acting transitively on Ω, where $|\Omega| > 1$. Then there is an element g of G that fixes no element of G (that is, $\chi(g) = 0$).

  Proof. Since the action is transitive, $\frac{1}{|G|}\sum_{g\in G}\chi(g) = 1$. So the average value of $\chi(g)$ is 1. However, $\chi(1) = |\Omega| > 1$, which is above average. Then there is a g where $\chi(g)$ is strictly below the average. This forces $\chi(g) = 0$. Since $\chi(g) \in \mathbb{N}\cup\{0\}$.

3 Sylow Subgroups

- **Freshman Arithmetic**: Let p be a prime. Then

$$(x+1)^p \equiv x^p + 1 (\mathrm{mod}\, p).$$

  Proof. Since

$$(x+1)^p = \sum_{k=0}^{p}\binom{p}{k}x^k \text{ and } \binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

  Therefore, the coefficients of x^k is divisible by p for all $0 < k < p$.

- **Lemma 5.1**: Let $n = p^a m$ where p is a prime. Then

$$\binom{n}{p^a} \equiv m \bmod p.$$

Proof. We have $(x+1)^{p^a} \equiv x^{p^a} + 1 (\bmod p)$ by repeatly using Freshman arithmetic. We have

$$(x+1)^n \equiv (x+1)^{p^a m} \equiv (x^{p^a}+1)^m (\bmod p).$$

We compute the coefficient of x^{p^a} on both sides. We have

$$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

and

$$(x^{p^a}+1)^m = \sum_{j=0}^{m} \binom{m}{j} (x^{p^a})^j.$$

The coefficient of x^{p^a} are $\binom{n}{p^a}$ and $\binom{m}{1} = m$, respectively. These must be congruent, so

$$\binom{n}{p^a} = m (\bmod p).$$

- **Theorem 5.2**: Let G be a finite group of order $n = p^a m$ where $p^a \nmid m$. Then G has a subgroup of order p^a.

Proof. Let Ω be the set of all subsets of G with cardinality p^a. Note $|\Omega| = \binom{n}{p^a}$. Let G act on Ω by right multiplication. We have $|\Omega| = \binom{n}{p^a} \equiv m \not\equiv 0 (\bmod p)$ (by lemma 5.1). So $p \nmid |\Omega|$, implying that some orbit $\mathcal{O}$ satisfies $p \nmid |\mathcal{O}|$. We have $|G| = |\mathcal{O}||G_x|$, where $x \in \mathcal{O}$. Since $p^a \big| |G|$, $p \nmid |\mathcal{O}|$, we have $p^a \big| |G_x|$, so $p^a \le |G_x|$. Note that for any $h \in G_x$, $Xh = X$. So $XG_x = X$, implying that $zG_x \subset X$ for any $z \in X$. Therefore, $|G_x| = |zG_x| \le |X| = p^a$. So $|G_x| = p^a$. Hence G_x is the desired subgroup.

Original proof.

1) If G satisfies Sylow E, for some p show all its subgroups do too.
2) Show that $GL(n,p)$, p is prime satisfies Sylow E (direct construction).
3) Use a form of Cayley's theorem to show any finite group is a subgroup of $GL(n,p)$ for some large enough n.

- **Example**: Show there is no simple group of order 100. By the Sylow-E theorem, G must have a subgroup H of order 25. Let G act on the 4 cosets of H. Let N be the kernel of the action. If G is simple, $N = \{1\}$. N can't equal G since G acts transitively on the cosets of H. Then G/N must be isomorphic to a subgroup of S_4. So $100|4!$, a contradiction.

- **Corollary 5.4 (Cauchy)**: Let G be finite with $p \big| |G|$, where p is prime. Then G has an element of order p.

Proof. Let p^a be the biggest power of p dividing $|G|$. Then G has a Sylow subgroup H of order p^a. Let $g \in H, g \neq 1$. Then $|g| \big| p^a$. So $|g| = p^e$ for some $1 \le e \le a$. We have $g^{p^{e-1}} \in H$, $g^{p^{e-1}} \neq 1$, $(g^{p^{e-1}})^p = 1$, so $|g^{p^{e-1}}| = p$.

- Sylow(G) = set of all Sylow-p subgroups of G. Notation: $n_p(G) = |\mathrm{Syl}_p(G)|$.

- **Midterm Exam**:

1) **Facts/short proofs**. Example: Let $|G| = 168$, $|H| = 24$. Suppose there is a $g \in G$ with $H^g = H$, and the $\sigma g = 7$. Is $H \lhd G$? Explain. Solution: We have $\mathbf{N}_G(H) \le G$. Also, $H \le \mathbf{N}_G(H)$, therefore, $24 \big| |\mathbf{N}_G(H)|$. Also, $g \in \mathbf{N}_G(H)$ so $|g| = 7$ divides $|\mathbf{N}_G(H)|$. We must have $|\mathbf{N}_G(H)| = 168$. Hence $H \lhd G$.
2) **Computations**. For example, given a concrete group, compute $\mathbf{C}_G(x)$, counting using Cauchy Frobenius theory, etc.
3) **Generic proofs**. Subgroup tests, show a subgroup is normal, isomorphism/non-isomorphism, homomorphism.
4) Tentative test date: 11:00 AM - 01:00 PM MST, March 24, 2017, Friday. Place remains to be decided.

- **Definition**: A group is called a p-group (p is prime) if every element of G has order a power of p.
- **Corollary 5.5**: A finite group is a p-group if and only if its order is power of p. $|G| = p^a m$, where p is prime, and $p \nmid m$.
- **Theorem 5.6 (Sylow D)**: Let G be finite, $P \subseteq G$ be a p-subgroup where $p \big| |G|$. Then there is an $S \in \mathrm{Syl}_p(G)$ with $P \subseteq S$.
- **Theorem 5.7 (Sylow C)**: Let G be finite, $p \big| |G|$. Then the set $\mathrm{Syl}_p(G)$ is a single conjugacy class of subgroups of G.
- **Theorem 5.8**: Let G be finite, P a p-subgroup of G. Let $S \in \mathrm{Syl}_p(G)$. Then there is an $x \in G$ with $P \subseteq S^*$.

  Proof. Let G, P, S be as given. Let $\Omega = \{Sx : x \in G\}$. Let P act on Ω by right multiplication. Then $|\Omega| = |G : S|$ which is not divisible by p. So some orbits has size not divisible by p, meaning the size of this orbit is 1. So P stabilizes some coset Sx. Then $Sxg = Sx$ for all $g \in P$. So $S^x g = S^x$ for all $g \in P$, forcing $P \subseteq S^x$.
- **Corollary 5.9**: Let $P \in \mathrm{Syl}_p(G)$. Then $n_p(G) = |G : \mathbf{N}_G(P)|$. In particular, $n_p(G) \big| |G|$. In other words, $|G| = p^a m, p \nmid m$, then $n_p(G) | m$.
- **Sylow Subgroups**: $|G| = p^e m, p \nmid m, e \geq 1$.
  - **Sylow E (power e)**: There is a subgroup of order p^e.
  - **Sylow C (conjugate)**: All Sylow-p subgroups are conjugate.
  - **Sylow D (development)**: Every p-subgroup is containted in a Sylow-p subgroup, $n_p(G) =$ number of Sylow-p subgroups. $\mathrm{Syl}_p(G) =$ set of Sylow-p subgroup.

    $$n_p(G) = \frac{|G|}{|\mathbf{N}_G(S)|} = |G : \mathbf{N}_G(S)|,$$

    where $S = \mathrm{Syl}_p(G)$ and $n_p(G) | m$.
- **Corollary 5.10**: Let $S \in \mathrm{Syl}_p(G)$. The following are equivalent:

  1) $S \lhd G$.
  2) S is the unique Sylow-p subgroup of G, ($n_p(G) = 1$).
  3) S contains every p-subgroup of G.
  4) $S \operatorname{char} G$.

  Proof.

  1) $\Rightarrow$ 2) We have $n_p(G) = |G : \mathbf{N}_G(S)| = |G : G| = 1$.
  2) $\Rightarrow$ 3) Let $P \subseteq G$ be a p-subgroup. Then $P \subseteq S^x$ for some x, so $P \subseteq S$, since S^x is equal to S (S^x is a Sylow-p subgroup too).
  3) $\Rightarrow$ 4) Let σ be an automorphism of G. Then $\sigma(S)$ is a Sylow-p subgroup of G, in particular, $\sigma(S)$ is a p-group, so $\sigma(S) \subseteq S$. Since $|S| = |\sigma(S)|$, we have $S = \sigma(S)$. Therefore $S \operatorname{char} G$.
  4) $\Rightarrow$ 1) All characteristic subgroups are normal.
- **Lemma 5.12**: Let $|G| < \infty$, $S \in \mathrm{Syl}_p(G)$. Let P be a p-subgroup of $\mathbf{N}_G(S)$. Then $P \subseteq S$.

  Proof. We have $S \in \mathrm{Syl}_p(\mathbf{N}_G(S))$, and $S \lhd \mathbf{N}_G(S)$, so S contains every p-subgroup of $\mathbf{N}_G(S)$.
- **Theorem 5.11**: Let $|G| = p^e m$, $p \nmid m$. Then $n_p(G) \equiv 1 (\mathrm{mod}\, p)$. In fact, $n_p(G) \equiv 1 (\mathrm{mod}\, p^t)$ if $p^t \leq |S : S \cap T|$ for all $S, T \in \mathrm{Syl}_p(G)$, $S \neq T$.

  Proof. Let $P \in \mathrm{Syl}_p(G)$, and let P act by conjugation on $\mathrm{Syl}_p(G)$. We note $\{P\}$ is an orbit of size divisible by p. Let $S \in \mathrm{Syl}_p(G)$, $S \neq P$. Let $\mathcal{O}$ be the orbit containing S. So $|\mathcal{O}| = |P : \mathbf{N}_P(S)|$. We have $\mathbf{N}_P(S) \leq \mathbf{N}_G(S)$ and $\mathbf{N}_P(S)$ is a p-subgroup of $\mathbf{N}_G(S)$. So $\mathbf{N}_P(S) \leq S \cap P$. Noting $S^g = S$ for each $g \in S \cap P$, we have $\mathbf{N}_P(S) = S \cap P$. Since $|\mathcal{O}| = |P : P \cap S|$ which is a (proper) power of p. So $p \big| |\mathcal{O}|$. Therefore, the orbits partition $\mathrm{Syl}_P(G)$ into sets of size a multiple of p together with $\{P\}$. The fact that $n_p(G) \equiv 1 (\mathrm{mod}\, p)$ follows.
- **Lemma 5.16**: Let $|G| = p^a m$, $p \nmid m$, $m > 1$. If G is simple,

  1) $n_p(G) | m$.

2) $n_p(G) = 1 (\mathrm{mod}\, p)$.
3) $|G| \big| (n_p(G))!$.

Proof. We show condition 3. let G act on $\mathrm{Syl}_P(G)$ by conjugatoin. Since G is simple, the kernel of the action is $\{1\}$ and G. If the kernel is G, $n_p(G) = 1$, so there is a normal $\mathrm{Syl}_P(G)$. If kernel is $\{1\}$, we have that G is isomorphic to a subgroup of $\mathrm{Sym}(\mathrm{Syl}_P(G))$. So $|G| \big| (n_p(G))!$.

- **Example**: $1,000,000 = 2^6 5^6$, $n_5(G) | 2^6$, $n_5(G) \equiv 1 (\mathrm{mod}\, 5)$, so $n_5(G) = 1, 16$, $10^6 \nmid 16!$.

3.1 finite p-groups

- **Lemma 5.20**: Let P be a finite p-group acting on Ω. Let $\Omega_0 = \{\alpha \in \Omega | \alpha \cdot x = \alpha, \forall x \in P\}$. Then $|\Omega| \equiv |\Omega_0| (\mathrm{mod}\, p)$.

  Proof. The set Ω_0 is the set of orbits of size 1. All other orbits must have size a mutiple of p. Since the orbits partition Ω, we have $|\Omega| \equiv |\Omega_0| (\mathrm{mod}\, p)$.

- **Theorem 5.21**: Suppose $\{1\} < N \lhd P$, P is a finite p-group. Then $N \cap Z(P) > \{1\}$.

  Proof. Let P act on N by conjugation. Let $\mathbf{N}_0$ be the set of elements of N fixed by every element of P. Note that $x^g = x$ for all $g \in P$ if and only if $x \in Z(P)$. Then $\mathbf{N}_0 = N \cap Z(P)$. So $|N| \equiv |\mathbf{N}_0| \equiv |N \cap Z(P)| \equiv (\mathrm{mod}\, p)$ by Lemma 5.20. So $p \big| |N \cap Z(P)|$, implying $N \cap Z(P) > \{1\}$. Letting $N = P$, we see that $Z(P) > \{1\}$.

- **Corollary 5.22**: If P is a finite simple p-group, then $|P| = p$. In particular, P is prime cyclic.

  Proof. If P is not abelian, its center is proper nontrivial and normal, so P is not simple. Suppose P is abelian. Then P contains an element g of order p. If $\langle g \rangle \neq P$, then $\langle g \rangle$ is a proper normal subgroup of P, so P is not simple. If $\langle g \rangle = P$, P is prime cyclic.

- **Corollary 5.23**: Let P be a finite, nontrivial, p-group. Then P has a subgroup of index p. Furthermore, this subgroup is normal.

  Proof. Let N be a maximal-normal subgroup of P (meaning there is no normal subgroup $M \lhd P$ with $N < M < P$). Then P/N must be simple (by the corresponding theorem). Since P/N is a p-group, it must have order p. Therefore, $|P : N| = p$.

- **Corollary 5.24**: Let $|G|$ be finite and $p^e \big| |G|$. Then G has a subgroup of order p^e.

  Proof. Let $|G| = p^a m$ where $p \nmid m$. Then G has a subgroup S of order p^a. Repatedly using Corollary 5.23, we see S has a subgroup of order p^e.

4 Permutation groups

- Recall $\mathrm{Sym}(X)$ is the collection of all permutations of X. And S_n is the permutation of number $1, \ldots, n$.
- **Disjoint cycle decomposition**: $(123)(378)(192)(765) = (2657839)$.
- **Lemma 6.3**: The order of a permutation is the least common multiple of its disjoint cycle lengths.
- **Example**: $(12345)^{(23)} = (23)(12345)(23) = (13245)$.
- **Lemma 6.4**: If g is an m-cycle, then g^n is an m-cycle for any permutation h. Furthermore, if $g = (\alpha_1, \ldots, \alpha_m)$, then $g^h = (\alpha_1 h, \alpha_2 h, \ldots, \alpha_m h)$.
- **Example**: $(123456)^{(356)} = (125463)$.
- **Example**: Let $x = (12)(345)$, $y = (52)(143)$ and we can find $g = (153)$ such that $y = x^g$.
- **Example**: $(123)(5789)^{(357)} = (125)(7389)$. And $(12)(345)^x = (35)(124)$ we have $x = (13)(254)$.
- **Theorem 6.5**: Two elements of $S_n(\mathrm{Sym}(X))$ are conjugate iff they have the same cycle structure.
- **Example**: For S_5, we have

Conjugate class	number
ϵ	1
(12)	$\binom{5}{2} = 10$
(123)	$2 \cdot \binom{5}{3} = 20$
$(12)(34)$	
(1234)	
$(12)(345)$	
(12345)	

- **Corollary 6.6**: For $n \geq 3$, $Z(S_n) = \{1\}$.

  Proof. Let $z \in Z(S_n)$. Then $z = z^g$ for all $g \in S_n$. If $z \neq \epsilon$, then z has some cycle of length ≥ 2. So $= z = (\alpha_1, \alpha_2, \cdots) \cdots$. Since $n \geq 3$, there is an $\alpha_3 \neq \alpha_1, \alpha_2$. Consider $z^{(\alpha_2, \alpha_3)} = (\alpha_1, \alpha_3, \ldots) \cdots$. However, $z, z^{(\alpha_2,\alpha_3)}$ don't map α_1 to the same element, so $z \neq z^{(\alpha_2,\alpha_3)}$, a contradiction. So $Z(S_n) = \{\epsilon\}$.

- **Definition** A transposition is a 2-cycle.

- **Lemma**: Every element of $S_n(\mathrm{Sym}(X))$ is a product of transposition.

  Why? $(\alpha_1, \alpha_2, \ldots, \alpha_m) = (\alpha_1, \alpha_2)(\alpha_1, \alpha_3) \cdots (\alpha_1, \alpha_m)$.

- **Corollary**: S_n is generated by transposition. In fact, it is generated by $(12), (13), \ldots, (1n)$ $(n-1$ total$)$.

- **Example**: $(1234) = (12)(13)(14)$.

- **Definition**: We call a permutation even if it can be written as a product of an even number of transposition. Odd if it can be written as an odd number of transpositions. Note: even cycle are odd, and odd cycles are even.

- **Lemma**: The identity can only be written as a product of an even number of transpositions.

  Proof. We use the following identities:

$$
\begin{aligned}
(ab)(ab) &= \epsilon \\
(ac)(ab) &= (ab)(bc) \\
(bc)(ac) &= (ab)(bc) \\
(cd)(ab) &= (ab)(cd)
\end{aligned}
$$

  Let $\epsilon = \beta_1 \beta_2 \cdots \beta_r$ where $\beta_1, \ldots, \beta_r$ are transpositions. We show r is even by induction. If $r \leq 2$, then r is even since clearly $r \neq 1$. Assume the assertion holds for $r < k$ for some integer k, where $k \geq 3$. Suppose $\epsilon = \beta_1, \beta_2, \ldots, \beta_k$. Consider $\beta_{k-1}\beta_k$ and some a moved by β_k. Using the identities, we can replace $\beta_{k-1}\beta k$ with $\beta'_{k-1}\beta'_k$, where a does not appear in β'_k. If $\beta'_{k-1} = \beta'_k$, then $\epsilon = \beta_1 \cdots \beta_{k-2}$, forcing $k-2$ to be even (induction hypothesis). Hence k is even. If not, a must be moved by β'_{k-1} and $\epsilon = \beta_1 \beta_2 \cdots \beta'_{k-1}\beta'_k$. We now repeat this on $\beta_{k-2}\beta'_{k-1}$. Either they cancel, and we're done by induction, or we can replace them with $\beta'_{k-2}\beta''_{k-1}$, where β''_{k-1} fixes a, but β'_{k-2} does not. Repeating this process, either there is cancellation at some point, forcing k to be even, or we have $\epsilon = \beta'_1\beta''_2 \cdots \beta''_{k-1}\beta'_k$, where $\beta''_2, \ldots, \beta''_{k-1}$ and β'_k all fix a, but β'_1 does not. Then β'_1 maps a to some other element b, but no other transpositions maps to anything to a. So $\beta'_1\beta''_2 \cdots \beta'_k$ does not fix a, a contradiction. So, by induction, if ϵ is a product of transpositions, then there must be an even number of them.

- **Theorem 6.8**: A permutation of S_n is even or odd, but not both.

  Proof. Let $g \in S_n$ and $g = t_1 t_2 \cdots t_m = s_1 \cdots s_l$ where $t_1, t_2, \ldots, t_m, s_1, \ldots, s_l$ are transpositions. Then $t_1 t_2 \ldots, t_m s_l \cdots s_1 = \epsilon$, so $m + l$ must be even. This forces $m \equiv l (\mathrm{mod}\, 2)$.

- **Corollary 6.10**: Let $n > 1$, then the set of even permutations in S_n form a norm subgroup of index 2 (note: called A_n).

  Proof. Note $\epsilon \in A_n$, so $A_n \neq \emptyset$. Let $x, y \in A_n$. Then x, y can be written as a product of an even number of transpositions. Therefore, xy^{-1} can be written as a product of an even number of transpositions. So $xy^{-1} \in A_n$. Therefore, $A_n \leq S_n$. Let $h, g \notin A_n$. Then ,hg^{-1} can be written as a product of an even number of transpositions. So $hg^{-1} \in A_n$, implying $A_n h = A_n g$. Then the only cosets of A_n are $A_n, A_n g$ for some $g \notin A_n$. Therefore, $|S_n : A_n| = 2$. Lastly, let $g \in S - N$, $h \in A_n$. Then $g^{-1}hg$ is a product of an even number of transposition, so $g^{-1}hg \in A_n$. Therefore, $A_n \lhd S_n$. (Also, the index $|S_n : A_n| = 2 \Rightarrow A_n \lhd S_n$.)

- **Permutation matrix**: Given $g \in S_n$, we define a matrix $P_g = (a_{ij})$ where $a_{ij} = \begin{cases} 1, & \text{if } g(i) = j \\ 0, & \text{otherwise.} \end{cases}$

- **Example**: $g = (12345) \in S_5$, then

$$P_g = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

  Let e_i be the $i$the elementary basis vector as a row vector in $\mathbb{R}^n$, then $e_1 P_g = e_2$, $e_2 P_g = e_3$. Can see that $P_g P_n = P_{gn}$, and $P_{g^{-1}} = (P_g^{-1} = P_g^T$. We have $\{P_g : g \in G\} \leq GL(n, \mathbb{R})$. Let $\phi : S_n \to GL(n, \mathbb{R})$ be defined by $\phi : g \mapsto P_g$. This is a homomorphism, injective $\ker = \{\epsilon\}$. Therefore, $S_n \cong GL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$. Let $\phi : GL(n, \mathbb{R}) \to \mathbb{R}$, $\psi(M) = \det M$. Consider $\phi \cdot \psi : S_n \to \mathbb{R}$. The image of $\phi \cdot \psi$ is $\{1, -1\}$. In fact, $\phi \cdot \psi(t) = -1$ for any transportations, so $\phi \cdot \psi(g) = 1$ for every even permutation g, $\phi \cdot \psi(g) = -1$ for every odd permutation g. Forcing $|S_n : A_n| = 2$ and since $A_n = \ker(\phi \cdot \psi)$, $A_n \lhd S_n$.

- **Corollary 6.11**: Let G act on Ω and suppose g induces an odd permutation on Ω. Then there is a normal subgroup A of G with $|G : A| = 2$.

  Proof. Let $\phi : G \to \{1, -1\}$ be defined by $\phi(g) = \det(P_g)$. We have image$(\phi) = \{-1, 1\}$ (since $\phi(g) = -1$). So $G/A \cong \{-1, 1\}$ where $A = \ker \phi$. Then $A \lhd G$, $|G : A| = 2$.

- **Example**: The permutation $(123)(1435)(87921)(375621)$ is even! We just look at the number of odd permutations. If the number is odd, then the permutation is odd, otherwise, the permutation is even.

- **Theorem 6.17**: A_n is simple for $n \geq 5$.

  Note: A_4 is not simple, $\{\epsilon, (12)(34), (13)(24), (14)(23)\} \lhd A_4$. A_3 is simple, $A_3 \cong \mathbb{Z}_3$. $A_2 = \{\epsilon\}$ is also simple.

- In 1800s, Holder came up with the idea:

  1) Find all finite simple groups (Done).
  2) Use this to find all finite groups (Very unrealistic).

5 Chapter 7 Direct product

- Recall that H, K are groups, $H \times K = \{(h, k) : h \in H, k \in k\}$, i.e. $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$.

- When is a group isomorphic to a direct product of groups?

- **Example**: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ (modulo under addition), and $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\} = \langle (1, 1) \rangle$. So $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ (just by mapping the generator of $\mathbb{Z}_6$ to the generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$.)

- How can we tell in general? In $H \times K$ define

$$\overline{H} = \{(h, 1) : h \in H\}, \overline{K} = \{(1, k) : k \in K\}.$$

  Note: $\overline{H} \cong H, \overline{K} \cong K$. We also have

$$\overline{H} \cap \overline{K} = \{(1, 1)\} \text{ and } \overline{HK} = H \times K \text{ and } \overline{H}, \overline{K} \lhd H \times K.$$

- **Idea**: Given a group G, look for subgroup H, K satisfying

$$H, K \lhd G; HK = G; H \cap K = \{1\}.$$

- **Example**: In $\mathbb{Z}_6$, take $H = \{0, 3\}$, $K = \{0, 2, 4\}$.
- If G has two such subgroups, we say G is the *internal direct product* of H and K. We write $G = H \odot K$.
- **Lemma 7.1**: Let $M, N \lhd G$, $M \cap N = \{1\}$. Then $mn = nm$ for each $m \in M$ and $n \in N$.
  Proof. Let $m \in M, n \in N$. And the commutator $[m, n] = m^{-1}n^{-1}mn = (n^{-1})^m n = m^{-1}m^n$. Since $M, N \lhd G$, $(n^{-1})^m n$ inN, $m^{-1}m^n \in M$, so $[m, n] \in M \cap N$. This forces $[m, n] = 1$. Note: $h_1k_1h_2k_2 = h_1h_2k_1k_2$.
- **Lemma 7.2**: If $G = H \times K$, then $G \cong \overline{H} \odot \overline{K}$. Also, if $\Gamma = M \times N$, then $\Gamma \cong M \times N$.
  Proof. (2nd part) Let $\theta : M \times N \to \Gamma$ via $\theta((m, n)) = mn$. We have

$$\theta((m_1, n_1)(m_2, n_2)) = \theta((m_1m_2, n_1n_2)) = m_1m_2n_1n_2 = m_1n_1m_2n_2 = \theta((m_1, n_1))\theta((m_2, n_2)).$$

  So θ is a homomorphism. Since $\Gamma = MN$, θ is surjective. Lastly,

$$\ker\theta = \{(m, n), m \in M, n \in n, \text{ and } mn = 1\}.$$

  If $mn = 1$, then $m = n^{-1}$, so $m \in M \cap N$, forcing $m = 1$. Similarly, $n = 1$. So $\ker\theta = \{(1, 1)\}$. Therefore, θ is an isomorphism as desired. Note: in general, internal direct product factors are not unique.
- **Example**: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle(1, 0)\rangle \odot \langle(0, 1)\rangle = \langle(1, 0)\rangle \odot \langle(1, 1)\rangle$.
- **Lemma 7.3**: If $G = M \odot N$, then $M \cong G/N$ and $N \cong G/M$.
  Proof. We have $G/N = MN/N \cong M/M \cap N \cong M$.
- **Lemma 7.4**: If $G = M \odot N = M \odot L$, then $N \cong L$.
- **More than two factors**: $G \times H \times K = \{(g, h, k) : g \in G, h \in H, k \in K\}$. Internal direct product: group Γ, subgroups $M_1, M_2, \ldots, M_n$ with $M_1, M_2, \ldots, M_n \lhd G$. Hence $G = \prod_{i=1}^{n} M_i$ and each element of G can be written uniquely as a product $m_1, \ldots, m_n$, where $m_i \in M_i$ for each $1 \le i \le n$.
- $(h, 1)^{(g,t)} = (h^g, 1^t) = (h^g, 1) \in \overline{H}$.
- **(External) direct product**: $\Gamma = X_{\alpha \in I} H_\alpha = \{(h_1, h_2, \ldots, h_\alpha, \ldots) : h_\alpha \in H_\alpha\}$.
- **(Internal) direct product**: $G = \prod_{i=1}^{n} M_i$ which means $M_1, M_2, \ldots, M_n \lhd G$, $G = M_1 \cdots M_n$, every element of G has a unique representation as $m_1 \cdots m_n$ where $m_i \in M_i$.
- **Theorem 7.5**: Let $M_1, \ldots, M_n \lhd G$, $\prod_{i=1}^{n} M_i = G$, the following are equivalent,

  1) $\prod_{i=1}^{n} M_i = G$.
  2) $M_i \cap \prod_{j \ne i} M_j = \{1\}$.
  3) $M_i \cap \prod_{j=1}^{i-1} M_j = \{1\}$.

  Proof.

  1) $\Rightarrow$ 2). Suppose $G = \prod_{i=1}^{n} M_i$, by way of contradiction, assume $M_i \cap \prod_{j \ne i}^{n} M_j > \{1\}$, let g be an element of this intersection, $g \ne 1$. Then $g = m_i$ for some $m_i \in M_i$. Also, $g = \pi_{j \ne i} m_j$ where $m_j \in M_j$. This violates the uniqueness of the representation of g.
  2) $\Rightarrow$ 3). Obvious.

3) $\Rightarrow$ 1). Assume 3) holds. Let $g \in G$, where $g = x_1 \cdots x_n = y_1 \cdots y_n$ where $x_i, y_i \in M_i$ for $1 \leq i \leq n$. By way of contradiction, assume $x_i \neq y_i$ for some i, where i is the largest such index. Then $x_1 \cdots x_i = y_1 \cdots y_i$. We have $x_i y_i^{-1} = (x_{i-1}^{-1} \cdots x_2^{-1} x_1^{-1})(y_1 y_2 \cdots y_{i-1}) \in \prod_{j=1}^{i-1} M_j$. Since $(x_{i-1}^{-1} \cdots x_2^{-1} x_1^{-1})(y_1 y_2 \cdots y_{i-1}) = y_1 x_1^{-1} y_2 x_2^{-1} \cdots y_{i-1} x_{i-1}^{-1}$ by Lemma 7.1. Then, $x_i y_i^{-1} \in M_i \cap \left(\prod_{j=1}^{i-1} M_j \right) = \{1\}$. So $x_i y_i^{-1} = 1$, giving $x_i = y_i$, contradiction. Therefore, each element has a unique representation so

$$G = \prod_{i=1}^{n} M_i.$$

- **Lemma 7.1** $G = \prod_{i=1}^{n} \mathbf{N}_i$, $\mathbf{N}_i = \prod_{j=1}^{m} M_{ij}$, then $G = \prod_{i,j} M_{ij}$.

  Proof. Clear $G = \prod_{i,j} M_{ij}$. Since the $\mathbf{N}_i$s all centralize each other. $M_{ij} \lhd G$ for i, j. Suppose $g = \prod_{i,j} x_{ij} = \prod_{i,j} y_{ij}$. Let $u_i = \prod_j x_{ij} \in \mathbf{N}_i$, $v_i = \prod_j y_{ij} \in \mathbf{N}_i$, so $g = \prod_i u_i = \prod_i v_i$ forcing $u_1 = v_1, \ldots, u_n = v_n$. For each i, $u_i = v_i$, so $\prod_j x_{ij} = \prod_j y_{ij} \in \mathbf{N}_i = \prod_j M_{ij}$, forcing $x_{ij} = y_{ij}$. Therefore, $G = \prod_{i,j} M_{ij}$.

- **Theorem 7.12**: Let G be a finite abelian p-group. Let C be a cyclic subgroup of max possible order in G. Then $G = C \times B$ for some $B \leq G$.

  Proof. If $C = G$, $B = \{1\}$, then we're done. Suppose $C < G$, we precede by induction on $|G|$. Choose $x \in G - C$, where $\sigma(x)$ is as small as possible. We have $\sigma(x^p) < \sigma(x)$, forcing $x^p \in C$. Note $\langle x^p \rangle \neq C$ ($|\langle x^p \rangle| < |\langle x \rangle|$). So x^p is a nongenerator of C. So $x^p = y^p$ for some $y \in C$. Then $xy^{-1} \notin C$, $(xy^{-1})^p = x^p y^{-p} = x^p (y^p)^{-1} = 1$. And $\sigma(x) \leq \sigma(xy^{-1}) = p$, so $\sigma(x) = p$. Let $X = \langle x \rangle$, $\phi : G \to G/X$ be the canonical homomorphism. We have $|X| = p$ and $X \not\leq C$, not $|C \cap X| = 1$. Then $\phi|_C : C \to \phi(C)$ is isomorphism. So $\phi(C)$ is a cycle in G/X of the same size as C. Then $\phi(C)$ is a cycle of largest order in G/X. By induction, $G/X = \phi(C) \times \phi(B)$, where $B \leq G$ with $X \leq B$. We claim $G = C \times B$. Note that $CB = G$, $C, B \lhd G$ and $C \cap B = \{1\}$. (Since $\phi(C \cap B) \subseteq \phi(C) \cap \phi(B) = \{1\}$, so $C \cap B \leq X$ and $C \cap X = \{1\}$). Therefore, $G = C \times B$. Repeating on B, we can write G as a indirect product of cyclic p-group.

- **Theorem 7.10**: Every finite abelian group is an internal direct product of cyclic p-groups.

  Proof. Let G be finite abelian group with $p_1, \ldots, p_n$ the distinct primes dividing $|G|$. Then $G = \prod_{i=1}^{n} S_i$ where S_i is a Sylow p_i-subgroup of G. By theorem 7.12, each group S_i is an internal direct product of cyclic p-group. By 7.11, G is an internal direct product of cyclic p-groups.

- **Corollary**: Every finite abelian *gp* is isomorphic to a direct product of cyclic p-groups.

- **Example**: Abelian groups of order of 8, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_8$. Note: Two abelian groups are isomorphic if and only if they have the same cyclic p-group "factors" in some order.

- **Example**; List all nonisomorphic abelian groups of order $200 = 2^3 \cdot 5^3$. $\text{Syl}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_4 = \mathbb{Z}_8$ and $\text{Syl}_5 = \mathbb{Z}_5 \times \mathbb{Z}_5 = \mathbb{Z}_{25}$. Then there are six possibilities:

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25} \\ \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ \mathbb{Z}_8 \times \mathbb{Z}_{25} \end{aligned}$$

  We have that if $\gcd(m, n) = 1$, $\mathbb{Z}_{m \times n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Hence $\mathbb{Z}_8 \times \mathbb{Z}_{25}$ is the only isomorphic abelian group.

mulplication	addition
$x \cdot x = x^2$	$x + x = 2x$
x^{-1}	$-x$
1	0

6 Rings and Ideals

- From now on, we'll write abelian groups additively.
- **Protypical example**: $M_n(\mathbb{C})$ - the set of all $n \times n$ complex matrices under addition and matrix multiplication.
- **Definition**: Let R be a set with two binary operations $+$ and $\cdot$, we call R a ring if

  1) R_+ is an abelian group.
  2) $\cdot$ is associative.
  3) $r(s+t) = rs + rt$.
  4) $(s+t)r = sr + tr$.
  5) There is an element $1 \in R$ such that $1 \cdot r = r \cdot 1 = r \forall r \in R$. Note: this element must be unique.

- Notes:

  1) Multiplication may not be commutative.
  2) Elements may not have multiplicative inverse.
  3) Multiplication cancellation may not hold.
  4) If R satisfies $1-4$ but not 5 call it a *rng*.
  5) Commutativeness of addition is implied by other axioms:

$$(r+s)(1+1) = r+r+s+s = r+s+r+s \Rightarrow r+s = s+r.$$

- **Example**:

  1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{A}, \mathbb{C}, \mathbb{H}$ – quaternion are rings.
  2) $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, where $i^2 = j^2 = k^2 = -1$, $ij = k, ji = -k$. Now consider

$$(a+bi)(j+k) = aj + ak + bij + bik = aj + ak + bk - bj = (a-b)j + (a+b)k.$$

  3) $\mathbb{H}$ is a division ring: every nonzero element has a (multiplicative) two sided inverses, not commutative.
  4) $M_n(\mathbb{R})$ - ring of all $n \times n$ matrices with entries from a ring R.
  5) External direct sums of rings,

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(r_1, r_2, \ldots, r_n) : r_1 \in R_1, r_2 \in R_2, \ldots r_n \in R_n\}.$$

  6) Polynomial rings: $R[x]$ - ring of polynomials with coefficients from the ring R, (assume multiplication commutes). Usually, require R is commutative.
  7) $\mathbb{Z} \oplus \mathbb{Z}$ is a ring with the multiplicative identity $(1, 1)$.

- **Subrings**: $S \subseteq R$ is called a subring if S forms a ring under the operations of R.
- **Example**: $S = \{0\} \oplus \mathbb{Z} = \{(0, a), a \in \mathbb{Z}\}$, S is a subring of $\mathbb{Z} \oplus \mathbb{Z}$, but it has a different multiplicative identity $(0, 1)$.
- **Example**: Let $\mathbb{Z}_6$ denote the ring of integers $(\mathrm{mod}\, 6)$, $S = \{0, 2, 4\}$ is subring of $\mathbb{Z}_6$ with the identity 4.
- **Subring**: $S \subseteq R$ is called a subrng if S forms a rng under the operations of R.
- **Example**: $2\mathbb{Z}$ is a subrng of $\mathbb{Z}$.
- **Lemma 12.3**: For $a \in \mathbb{R}$, recall that $-a$ is the additive inverse of a. In a ring we have:

1) $0 \cdot r = 0 = r \cdot 0, \forall r \in R$.
2) $(-r)s = -(rs) = r(-s), \forall r, s \in R$.
3) $-(-r) = r, \forall r \in R$.

Proof.

1) Let $r \in R$, we have
$$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0.$$
Then,
$$-(r \cdot 0) + r \cdot 0 = -(r \cdot 0) + r \cdot 0 + r \cdot 0,$$
implying $0 = r \cdot 0$. $0 \cdot r = 0$ is similar.
2) Let $r, s \in R$, then $0 = 0 \cdot s = [r + (-r)] \cdot r = r \cdot s + (-r) \cdots s$. This implies $-(rs) = (-r)s$. Similarly, we have $r(-s) = -(rs)$.

- **Definition**: $I \subseteq R$ Iis called an ideal of R if

1) I is an additive subgroup of R.
2) $\forall a \in I, r \in R, ra \in I$ and $ar \in I$.

- **Example**: $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Note: an ideal is a subrng with the *absorption property* $\forall a \in I, \forall r \in R, ar, ra \in I$. Put another way: $rI \subseteq I, Ir \subseteq I$.

- **Example**:

1) $\mathbb{Z}[x], I = \{f \in \mathbb{Z}[x] : f(1) = 0\} = \{(x-1)g : g \in \mathbb{Z}[x]\}$, this ideal has the form $(x-1)\mathbb{Z}[x]$.
2) Let $J = \{g \in \mathbb{Z}[x] : g(0) \text{ is even.}\}$, ideal, not principal.

- If R is commutative ring and $a \in R$, then aR is the ideal of R. Called *principal ideals*.

- In non-commutative rings, we can weaken the definitoin of ideal, replacing the absorption property with either $\forall a \in I, r \in R, ar \in I$ or $\forall a \in I, r \in R, ra \in I$ called right and left ideals respectively.

- **Example**: In $M_n(R)$, let S be the set of upper triangular matrices. Is S an ideal?

- **Definition**: Ring homomorphism is a map $\theta : R \to S$ satisfying
$$\begin{cases} \theta(s + r) = \theta(s) + \theta(r) \\ \theta(sr) = \theta(s)\theta(r) \end{cases}$$
and $\ker(\theta) = \{r \in R | \theta(r) = 0\}$.

- **Lemma 12.4**: Let $\theta : R \to S$ be a ring homomorphism with $\ker(\theta) = I$. Then I is an of ideals of R.

Proof. Since θ is also a group homomorphism, it's clear that $\ker\theta = I$ is an additive subgroup of R. Let $a \in R$ and $r \in R$. Then $\theta(ar) = \theta(a)\theta(r) = 0 \cdot \theta(r) = 0$. So $ar \in I$. Similarly, $ra \in I$. Therefore, I is an ideal of R.

- **Examples**:

1) (Trivial): $\theta : R \to S, \theta(x) = 0, x \in R$.
2) $\theta : \mathbb{Z} \to \mathbb{Z}_6$ via $\theta(x) = x (\mathrm{mod}\, 6)$.
3) $\theta : M_n(\mathbb{C}) \to \mathbb{C}$ via $\theta(A) = \det(A)$, this is not a homomorphism.
4) $\theta : M_n(\mathbb{C}) \to \mathbb{C}$ via $\theta(A) = \mathrm{tr}(A)$, this is not a homomorphism as well.
5) $\theta : \mathbb{R}[x] \to \mathbb{R}$ via $\theta(f) = f(2)$ is a homomorphism, called evaluation homomorphism.
6) Let T be the set of $n \times n$ upper triangular complex matrices, it forms a ring. Let $\theta : T \to T$ via
$$\theta(T) = \begin{bmatrix} T_{11} & 0 & \cdots & 0 \\ 0 & T_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$
Yes, it is a ring homomorphism.

- **Definition**: Quotient (factor) rings. Let R be a ring, I an ideal of R. R/I - set of additive cosets of I with the operation
$$r+I+s+I=(r+s)+I \quad \text{and} \quad (r+I)(s+I)=rs+I.$$
- **Example**: In $\mathbb{Z}$, $5\mathbb{Z}$ is an ideal. Then $\mathbb{Z}/5\mathbb{Z}=\{5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$.
- **Lemma 12.5**: R/I is a ring.

  Proof. From our work with groups, we know R/I is an additive group. We show the multiplication defined on R/I is well-defined. Suppose $r+I=r'+I$ and $s+I=s'+I$, then $r=r'+u$, $s=s'+v$ for $u,v\in I$. We have
$$\begin{aligned}(r+I)(s+I) &= rs+I\\ &= (r'+u)(s'+v)+I\\ &= r's'+r'v+us'+uv+I\\ &= r's'+I\\ &= (r'+I)(s'+I)\end{aligned}$$
  Lastly, the distributive law, associativity, multiplication are clear, and $1+I$ is the multiplicative identity of R/I.
- The canonical homomorphism $\theta: R\to R/I$ defined by $\theta(r)=r+I$, $\ker(\theta)=I$.
- **Corollary 12.6**: The ideals of R are precisely the kernels of homomorphism from R to (other) rings.
- **Lemma 12.7**: Let $\theta: R\to S$ be a surjective homomorphism. Let $I=\ker(\theta)$. Then $S\cong R/I$ (ring isomorphism).

  Proof. Define $\phi: R/I\to S$ via $\phi(r+I)=\theta(r)$. We already showed in 3.3 that this is well-defined group isomorphism. We now show
$$\phi((r+I)(s+I))=\phi(r+I)\phi(s+I)=\phi(rs+I)=\theta(rs)=\theta(r)\theta(s)=\phi(r+I)\phi(s+I).$$
- **Corollary**: Let $\theta: R\to S$ be a ring homomorphism, $\ker(\theta)=I$. Then $R/I\cong\theta(R)$.
- **Definition**: Unit in a ring. We call $x\in R$ a unit if there is an element $y\in R$ with $xy=yx=1$. Note 0 is only a unit of $R=\{0\}$.
- **Example**:

  1) Units in $M_n(\mathbb{C})$ are $GL(n,\mathbb{C})$ not subring, subrng.
  2) Units in $\mathbb{Z}$ is ± 1.
- **Definition**: A division ring is a ring where every nonzero element is a unit.
- **Definition**: A commutative division ring is called a field.
- **Lemma 12.8 (Correspondence theorem for rings)**: Let $\theta: R\to S$ be surjective ring homomorphism. Then θ determines a bijection between additive subgroups of R containing $\ker(\theta)$ and additive subgroups of S. Furthermore, under this correspondence, ideals of R containing $\ker(\theta)$ correspondent to ideals of S. Similarly, for left/right ideals.
- **Notes**: In general, if θ is surjective, $I\subseteq R$ is an ideal, so is $\theta(I)$. Also, if I is an ideal, so is $\theta^{-1}(I)$ (surjectivity is not needed).
- **Definition**: An element $x\in R$ is said to be a unit of R provided that there is some $y\in R$ such that $xy=yx=1$.
- Can also have elements with inverse on one side $ab=1$ - right inversie of a, $\nexists x$ with $xa=1$. Suppose $ab=bc=1$, $a=a(bc)=(ab)c=c$. So if an element has a left and right inverse in a ring, they are the same and it's a unit.
- Given R a ring the set of units in R, denoted $U(R)$ is a group under multiplication $\cdot$.
- **Group ring**. Let G be a multiplicative groups, finite. Let $\mathbb{F}$ be a field. Form set $R=\{\sum_{i=1}^{n} a_i g_i : a_i\in\mathbb{F}, i=1,\dots,n\}$.

- **Example**: $\mathbb{Z}_3$ written multiplicatively: $1, g, g^2, g^3 = 1$. Let $\mathbb{F} = \mathbb{R}$. New ring: $\{a + bg + cg^2, a, b, c \in \mathbb{R}\}$. Now consider

$$(a + bg + cg^2)(a' + b'g + c'g^2) = (aa' + bc' + cb) + (ab' + ba' + cc')g + (ac' + bb' + ca')g^2.$$

- **Lemma 12.10** Let I be a one-sided or two-sided ideal. Then $I = R$ if and only if I contains a unit.

  Proof. Let $I \subseteq R$ be (left/right) ideal. Without loss of generality, assume I has the left absorption property, i.e. $rI \subseteq I, \forall r \in R$.

  ($\Rightarrow$) If $I = R, 1 \in I$, so I contains a unit.

  ($\Leftarrow$) If I contains a unit u, and $x \in R$, we have $(xu^{-1})I \subseteq I$, so $xu^{-1}u \in I$, implying $x \in I$. Therefore $I = R$.

- **Corollary 12.11**: Let R be a nontrivial ring (note: $R = \{0\}$ is trivial). The following are equivalent:

  1) R is a division ring.
  2) The only right ideals are O, R.
  3) The only left ideals are O, R.

  Proof.

  1) $\Rightarrow$ 2), 3): Lemma 12.10.
  2) $\Rightarrow$ 1). Suppose R is a rignt whose only right ideals are O, R. Let $a \in R, a \neq 0$. We have aR is a right ideal. Since $a \in aR$, $aR \neq \{0\}$, so $aR = R$. Then $1 \in aR$, so $\exists b \in R$ with $ab = 1$. Repeating with bR, we see there is an element c with $bc = 1$. So $a = c$, and $ab = ba = 1$, implying a is a unit. Therefore R is a division ring.

- **Definition**: An ideal $I \subseteq R$ is called proper if $I \neq R$. We say I is a maximal ideal if I is proper and whenever J is an ideal with $I \subseteq J \subseteq R$, then $J = I$ or $J = R$. (That is, no proper ideal of R properly contains I).

- **Corollary 12.12**: A commutative ring R is a field if and only if $\{0\}$ is a maximal ideal.

- **Partial orders**: relation $\leq$ on a set A.

  1) $x \leq x$ (reflective).
  2) $x \leq y, y \leq x \Rightarrow x = y$ (anti-symmetric).
  3) $x \leq y, y \leq z \Rightarrow x \leq z$ (transitive).

- **Example**: subset relation on some power set. $\{1, 3\}$ and $\{2, 3\}$ are incomparable.

- **Fields**: $\mathbb{Q}[i] = \{a + bi, a, b \in \mathbb{Q}, i^2 = -1\}$, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$.

- Partial ordering is called total ordering if it also satisfies

  4) $\forall x, y \in A$, we have $x \leq y$ or $y \leq x$.

- A chain of a poset A is a totally ordered subset of A.

- **Example**:

  1) Let $\mathbb{N}$ be a set, P is the power set of $\mathbb{N}$. P is partially ordered by $\subseteq$.
  2) $\{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots\}$ is a chain.

- Let A be a poset, $B \subseteq A$, we say $u \in A$ is an upper bound for B provided that $\forall x \in B, x \leq u$.

- **Example**: $A = \mathbb{R}$, $B = (0, 1)$, an upper bound for B is 1.,

- **Definition**: An element m of B is called maximal if m is an upper bound for B and $m \in B$. That is, $\forall x \in B$, $m \in x$ implies $m = x$.

- **Zorn's Lemma**: If A is a nonempty poset and every chain of A has an upper bound, then A has a maximal element. That is, $\exists m \in A$ such that $\forall x \in A$, $m \leq x$ implies $m = x$.

  Proof. Equivalent to Axiom of Choice.

- **Example**: $A = (0, 1)$ ordered by $\leq 1 - \frac{1}{n}$? No, doesn't have maximal element.

- **Example**:

  1) $\mathbb{N}$ ordered by divisibility call $a \preccurlyeq b$ means $a|b$. $2 \preccurlyeq 10$, $2 \not\preccurlyeq 5$ (incomparable).
  2) $\mathbb{N}$, P is the power set of $\mathbb{N}$, the maximal element is $\mathbb{N}$.

- **Lemma 12.13**: Let R be a rinig, and $I \subseteq R$ a proper ideal. The I is contained in a maximal ideal of R.

  Proof. Let I be a proper ideal and P the set of all proper ideals containing I, partially ordered by inclusion. Let C be a chain in P. Let $J = \bigcup_{A \in C} A$. We claim J is also a proper ideal of $x, y \in K$, for some $K \in C$. Then $x - y \in K \subseteq J$. So J is an additive subgroup of R. Let $x \in J$, $r \in R$, then $x \in K$ for some $K \in C$ and $rx, xr \in K \subseteq J$, since K is an ideal. Therefore, J is an ideal. However, J is proper since $1 \notin K$ for any $K \in C$, implying $1 \notin J$. By Zorn's Lemma, P has a maximal element. The theorem follows.

- **Corollary 12.14** If R is nontrivial commutative ring, then there is a surjective homomorphism from R to a field.

  Proof. $\{0\}$ is an ideal of R, so it is contained in a maximal ideal of R. Call this ideal I, by the correspondence theorem, the ideal of R/I corresponds to the ideals of R that contain I. Since I is maximal, the only ideals of R contain I are R, I. So the only ideals of R/I are $\{1\}$ (the trivial one) and R/I. Since the trivial ideal is maximal in R/I, R/I is a field.

- **Definition**: A ring is called simple if its only 2-sided ideals are R, $\{0\}$.

- **Theorem 12.15**: Let D be a division ring. Then $M_n(D)$ is simple.

  Proof. Suppose $I \subseteq M_n(R)$ is a nontrivial ideal, that is, $I \neq \{0\}$. Then $\exists A \in I$, $A \neq 0$, say $A_{ij} \neq 0$. Then

  $$\frac{1}{A_{ij}} e_{ki} A e_{jl} = e_{kl} \text{ for } k, l, e_{ij} e_{kl} = \begin{cases} 0 \text{ if } j \neq k \\ e_{il} \text{ if } j = k \end{cases}.$$

  So $e_{k,l} \in I$ for all k, l, so $I = M_n(D)$.

- **Example**: Some polynomial rings.

  1) $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$, provided that $\mathbb{Q}[x]$ is polynomial ring.
  2) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ for the polynomial ring $\mathbb{Z}[x]$.
  3) $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Z}\}$ for the polynomial ring $\mathbb{Z}[x]$.
  4) $\mathbb{R}[i] = \mathbb{C}$.

- Suppose we want all solutions to $y^2 = 2x^2$, where $x, y \in \mathbb{Z}$. The only solution is $x = y = 0$.

  Proof. Suppose x, y are solutions, $x, y \neq 0$. Without loss of generality, $x, y > 0$, we have the following prime factorization,

  $$x = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad y = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m},$$

  where $p_i, q_j, i = 1, 2, \ldots, n, j = 1, 2, \ldots, m$ are primes and $a_i, i = 1, 2, \ldots n$ and $b_j, j = 1, 2, \ldots, m$ are integers. Hence,

  $$y^2 = 2x^2 : q_1^{2b_1} q_2^{2b_2} \cdots q_m^{2b_m} = 2 \cdot p_1^{2a_1} p_2^{2a_2} \cdots p_n^{2a_n}.$$

  Since the order of 2 is odd, hence this does not hold.

- **Fermat's last theorem**: $a^n + b^n = c^n$, $n \geq 3, n \in \mathbb{Z}$.

- $x^2 - x = y^3 \Rightarrow x(x-1) = y^3$, this gives $x = 0, 1, \quad y = 0$. Suppose $x > 1$, $\text{GCD}(x, x-1) = 1$. So $x = n^3, x - 1 = m^3$, but $n^3 > m^3$, note that

  $$(m+1)^3 = m^3 + 3m^2 + 3m + 1 > m^3 + 1 = xn^3.$$

  This yields, $(m+1)^3 > n^3 > m^3$, which is impossible. Similar for $x < 0$.

- Find all integer solutions: $y^3 = x^2 + 2$, we have $x = \pm 5, y = 3$. We can find the unique factorization "irreducibles".

  $$y^3 = (x + \sqrt{2})(x - \sqrt{2}) \in \mathbb{Z}[\sqrt{-2}].$$

- **Example**: $\mathbb{Z}[\sqrt{-d}]$ has unique factorization if and only if $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ where d is square-free.

7 Chapter 16: Commutative rings

- **Integral domain**: for $\forall a, b \in R$, if $ab = 0$ when $a = 0$ or $b = 0$ (commutative).
- **Example**: $\mathbb{Z}_p$ is an integral domain, where p is prime.
- **Definition**: An ideal of a (commutative) ring is called principal if it is of the form $(a) = \{ar : r \in R\}$.
- $\mathbb{Z} : (2), (3), \ldots$ every ideal of $\mathbb{Z}$ is principal "principal ideal ring" (PIR), "principal ideal domain" (PID).
- $\mathbb{Z}[x]$, this is an integral domain. Is it a PID? No. $I = \{f \in \mathbb{Z}[x] : f(0) \text{ is even. }\}$. Not a principal ideal.
- **Lemma 16.1**: Let S be a unitary overing in R (contains R, has same multicative identity). Then the map $\phi : R[x] \to S$ via $\phi(f) = f(s)$ is a homomorphism. $\phi : \mathbb{Q}[x] \to \mathbb{C}$ by $\phi(f) = f(i)$, and the image of ϕ is $\mathbb{Q}[i]$. The kernel of ϕ is $(x^2 + 1)$. By isomorphism theorem, we have $Q[x]/(x^2 + 1) \cong \mathbb{Q}[i]$.
- **Degree of nonzero polynomial**: the order of the highest degree term.
- **Example**:

  1) $\deg(3x^7 - 5x) = 7$.
  2) In $\mathbb{Z}_6$, we have $\deg([(2x + 3)(3x + 5)]) = 1$, $\deg([(3x + 3)(2x + 2)]) = 0$.

- **Lemma 16.2**: Let $f, g \in R[x]$ have degrees m, n and leading coefficient a, b. If $a, b \neq 0$, the $\deg(fg) = m + n$. Also,

  1) If R is a domain, so is $R[x]$.
  2) If f, g are monic (leading coefficient 1), then so is fg.

- **Lemma 16.3 (Division algorithm)**: Let $f, g \in R[x], f \neq 0$. Assume the leading coefficient of f is a unit. Then there exist $q, r \in R[x]$ with $g = fg + r$ where $r = 0$ or $\deg(r) < \deg(f)$. Note if R is a field, leading coefficient of f is always a unit $\mathbb{Q}[x]$.
- **Example**: $g = x^3 + 2$, $f = 2(x - 1)$, then $x^3 + 2 = \frac{1}{2}(x^2 + x + 1) \cdot 2(x - 1) + 3$.
- **Definition**: We say $a \in R$ is a zero divisor provided that $a \neq 0$ and there is $a, b \neq 0$ with $ab = 0$.
- **Lemma 16.4**: Let F be a field, then $F[x]$ is a PID.

  Proof. By 16.2, we know $F[x]$ is a domain. Let A be an ideal of $F[x]$. If $A = \{0\}$, done. If not, let f be a polynomial in A of smallest possible degree. Let $g \in A$, then there are $q, r \in F[x]$ with $g = fg + r$ and $\deg(r) < \deg(f)$ or $r = 0$. We cannot have $\deg(r) < \deg(f)$ by the minimality of f. So $r = 0$ and $g \in (F)$. This implies $A = (f)$.

- **Definition**: An element $a \in R$ is called irreducible if a is not a unit and whenever $a = bc$, we must have b is a unit or c is a unit.
- **Example**:

  1) Irreducibles in $\mathbb{Z}$: $\pm p$ where p is a prime number.
  2) Irreducibles in $\mathbb{C}$: degree 1 polynomials.
  3) Irreducibles in $\mathbb{R}[x]$: degree 1 polynomials and degree 2 polynomials with complex roots.

- **Lemma 16.5**: Let a, b, x, y be elements of R where R is a domain.

  1) If $ax = ay, a \neq 0$, then $x = y$.
  2) If $a|b$ and $b|a$, then $b = au$ for some unit u. Note: $a|b$ means that $b = ak$ for some $k \in R$. Only used for $a \neq 0$.

  Proof.

  1) If $ax = ay$, then $a(x - y)$. Since $a \neq 0$, R is a domain, we have $x - y = 0$.
  2) Suppose $a|b, b|a$, then $b = ak, a = br$ for $k, r \in R$. Then $b = brk$, so $1 = rk$. So $b = ak$ where k is unit.

- **Definition**: An element $p \in R$ is called prime if p is a nonzero, non-unit and whenever $p|ab$ then $p|a$ or $p|b$.
- **Example**: In $\mathbb{Q}[x]$, is $x^2 + 1$ prime? Yes.

- **Lemma 16.8**: Let R be a domain.

  1) If a is prime, then a is irreducible.
  2) If a is prime, and $a|b_1 \cdots b_n$, then $a|b_i$ for some i.
  3) Suppose $a_1 \cdots a_n = ub_1 \cdots b_m$ where a_is are prime, and b_is are irreducible, u a unit. Then, after reordering, $a_i = b_i u_i$ for a unit u_i, and $n = m$.

  Proof.

  1) Let $a \in R$ be prime, $b, c \in r$ be such that $a = bc$. Since $a|a$, so $a|bc$. Since a is prime, $a|b$ or $a|c$. Without loss of generality, $a|b$, then $b = ak$ for some $k \in R$. So $a = akc$. Then $1 = kc$. So c is a unit.
  2) Easy induction.
  3) By 2), since $a_1|ub_1 \cdots b_m$, we must have $a_1|b_i$ for some i, (a_1 cannot divide u, since only units divide units.) Then, without loss of generality, $a_1|b_1$. We have $b_1 = a_1 u_1$, where u_1 must be a unit, since b_1 is irreducible. Cancelling, we obtain $a_2 \cdots a_n = (u_1^{-1}u)b_2 \cdots b_m$. Now use induction.

- Note:

  1) **irreducible**: nonzero, non-unit a, if $a = bc$, then b or c is a unit.
  2) **prime**: nonzero, non-unit a, if $a|bc$, then $a|b$ or $a|c$.

- A ring is noetherian if every ascending chain of ideals in R is eventually constant. That is, if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. Then for some k, $I_n = I_k$ for all $n \geq k$.

- **Example**: $(k) = k\mathbb{Z}$. If $n\mathbb{Z} \subseteq m\mathbb{Z} \subseteq k\mathbb{Z}$, $n|m|n$.

- **Theorem**: A ring is noetherian if and only if every ideal is finitely generated.

  Proof. ($\Leftarrow$) Asumme every ideal is finitely generated. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals. Let $I = \bigcup_{k=1}^{\infty} I_k$, then I is an ideal, so I is finitely generated, meaning $I = (a_1, a_2, \ldots, a_n)$, for some $a_1, a_2, \ldots, a_n \in R$. Since $I = \bigcup_{k=1}^{\infty} I_k$, $I_1 \subseteq I_2 \subseteq \cdots$, there is some m with $a_1, \ldots, a_m, \ldots, a_n \in I_m$. Then $I \subseteq I_m \subseteq I_{m+1}$ forcing $I = I_m = I_{m+1} = \cdots$ Therefore, R is noetherian. ($\Rightarrow$) Suppose R is noetherian. Let I be an ideal, and form an ascending chain as follows. Pick $a_1 \in I_1$, define $I_1 = (a_1)$. If $I_1 = I$, I is finitely generated. If not, pick $a_2 \in I - I_2$, define $I_2 = (a_1, a_2)$. If $I_2 = I$, then I is finitely generated. If not, pick $a_3 \in I \backslash I_2$, define $I_3 = (a_1, a_2, a_3)$. Eventually, this chain must end (because noetherian). So for some n, $I = (a_1, \ldots, a_n)$ meaning it is finitely generated.

- **Definition**: Let $I \in R$ be an ideal. We say I is finitely generated if T here are elements $a_1, \ldots, a_n$ such that $I = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n : r_1, r_2, \ldots, r_n \in R\}$. We write $I = (a_1, \ldots, a_n)$.

- **Example**: Not noetherian rings: $\mathbb{Z}[x_1, x_2, \ldots, x_n], (x_1) \subseteq (x_1) \subseteq (x_1, x_2) \subseteq \cdots$.

- **Lemma 16.6**: Let R be noetherian, then every element of R is O, a unit, or a product of irreducibles.

  Proof. Let $X \subseteq R$ be the set of all nonzero, non-unit that are not product of irreducibles. By way of contradiction, assume $X \neq \emptyset$, let $\updownarrow = \{(x) : x \in X\}$. Also, $\updownarrow$ musst contain a maximal element, since R is noetherian. (maximal in $\updownarrow$). Call the maximal element (m). Since $m \in X$, m is not a product of irreducibles, so $m = ab$ where a, b are not units and not irreducible. So $m \in (a)$, so $(m) \in (a)$ implying $(m) = (a)$. So $a|m, m|a$, implying $m = an$, where u is a unit. So b in a unit, contradiction.

- **Lemma 16.9**: Let R be a PID, and let $a \in R$ and $a \neq 0$. The following are equivalent:

  1) a is prime.
  2) a is irreducible.
  3) (a) is maximal.

  Proof.

  1) $\Rightarrow$ 2) Lemma 16.8 a)

2) $\Rightarrow$ 3) Let a be irreducible, since a is not a unit, $1 \notin (a)$, so (a) is proper. Let I be an ideal, $(a) \subseteq I$. Since R is a PID, $I = (b)$ for some $b \in R$. Since $a \in (b)$, $a = bx$ for some $x \in R$. Since a is irreducible, either b or n is a unit, $b = ax^{-1} \in (a)$, so $(b) \subseteq (a)$. Then $(a) = (b)$. Therefore (a) is maximal.
3) $\Rightarrow$ 1) Suppose (a) is maximal, then (a) is a nonzero, nonunit (else $(a) = R$). Let $a|xy$. Since (a) is maximal, $R/(a)$ is a field. Note that $(x + (a))(y + (a)) = xy + (a) = (a)$. Since $R/(a)$ is a field, it is an integral domain, so $x + (a) = (a)$ or $y + (a) = (a)$. Therefore, $a|x$ or $a|y$.

- **Definition**: A domain is UFD (unique factorization domain) provided that

  1) Every nonzero, non-unit is a product of irreducibles.
  2) This factorization is unique, in that $a_1a_2 \cdots a_n = b_1b_2 \cdots b_m$, where $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m$ are irreducibles, implies that, after reordering, we have $n = m$ and $b_i = a_iu_i$ for units $u_1, \ldots, u_m$.

- **Example**: $\mathbb{Z}[x], \mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}]$ are UFDs, however, $\mathbb{Z}[\sqrt{-5}]$ is not.

- **Theorem 16.10**: Let R be a PID, then R is a UFD.

  Proof. Note that every ideal of R is principal, hence finitely generated. So R noetherian. This implies that every nonzero non-unit of R is factorable into irreducibles. Suppose $a_1a_2 \cdots a_n = b_1b_2 \cdots b_m$, where $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m$ are irreducibles. Then $a_1, \ldots, a_n, b_1, \ldots, b_m$ are all prime by Lemma 16.9, so 16.8 c show that $n = m$, (after reordering), $a_i = b_iu_i$ for $i \leq i \leq u$. Therefore, R is a UFD.

- **Example**: $\mathbb{Z}[x]$ is a UFD, but not a PID. Also, $\mathbb{Z}[x_1, x_2, \ldots]$ is UFD, not noetherian, for countably infinitely number of variables.

- **Lemma 16.11**: Let R be a UFD. Then, irreducibles are prime.

  Proof. Let $a \in R$ be irreducible and R a UFD. Suppose $a|xy$ for $x, y \in R$, $x, y \neq 0$, x, y not units. (if x is a unit, then $a|y$). Then $xy = ab$ for some $b \in R$. Note that b is also a nonzero, nonunit (since a is irreducible). So x, y, b can be written as products of irreducible, $ab_1 \cdots b_n = x_1 \cdots x_s y_1 \cdot y_t$. Since R is a UFD $a = u_ix_i$, $a = u_iy_i$ for some unit u_i. Then $a|x$ or $a|y$ implying a is prime.

- **Definition**: An ideal of a ring R is called prime if it is proper and whenver $xy \in I$ we have $x \in I$ or $y \in I$. Note: The principal ideal (a) is prime if and only if a is prime.

- **Lemma**: Let $I \subseteq R$ be an ideal. Then R/I is an integral domain if and only if I is prime.

  Proof. $\Rightarrow$ Suppose R/I is a domain, let $ab \in I$. We have $(a + I)(b + I) = ab + I = I$. Then $a + I = I$ or $b + I = I$ since R/I is a domain. Then $a \in I$ or $b \in I$, so I is prime.

- **Field of Fractions**: Let R be an integral domain. For $a, b \in R, b \neq 0$, create a "fraction" $\frac{a}{b}$ (formally ordered pair (a, b)). Define equivalence on fractions, where $ad = bc$. This is an equivalence relation. Let F be the set of inequivalent fractoins under the operations:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

  Then F is a field, called the field of fraction of R.

- **Example**: field of fractions $\mathbb{Q}[x]$ and $\mathbb{Q}(x)$ (rational functions).

- **Theorem 16.12**: If R is a UFD, so is $R[x]$.

- **Example**: $\mathbb{Z}$, $\mathbb{Z}[x]$. $3x^2 - 27 = 3(x + 3)(x - 3)$.

- **Theorem 16.17**: Similarly, so is $R[x_1, x_2, \ldots, x_n]$.

- **Definition**: Let R be a UFD. A primitive polynomial f is a polynomial such that the only elements of R dividing f are the units of R.

- **Example**: $3x^2 - 15x + 2$, $x^3 + x + 2$.

- **Lemma 16.13**: Let R be UFD, a primitive nonconstant polynomial in $R[x]$ is irreducible if and only if it cannot be factored into two constant polynomials of lesser degree.

- **Definition**: R - UFD: irreducibles in $R[x]$ are

- irreducibles of R.
- primitive, nonconstant polynomials that can't be factored into lesser degree polynomials.
- Units of $R[x]$: units of R.

- **Lemma**: Let R be a UFD. The product of primitive polynomials is also primitive.

  Proof. Let $f, g \in R[x]$, f, g primitive. Suppose $f, g = ah$, where $a \in R$, a irreducible (hence prime). Let $\bar{R} = R/(a)$. Then $\bar{R}$ is an integral domain. Define $\phi : R[x] \to \bar{R}[x]$ so that $\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = (a_n + (a))x^n + \cdots + (a_0 + (a))$. This can be seen to be ring homomorphism (routine). We have $\phi(fg) = 0$, so $\phi(f)\phi(g) = 0$. Since $\bar{R}$ is an integral domain, so is $\bar{R}[x]$, implying $\phi(f) = 0$ or $\phi(g) = 0$. This means $a|f$ or $a|g$, this contradicts the fact they are primitive.

- **Lemma 16.14**: R-UFD. Let f be a nonconstant polynomials in $R[x]$. Then $f = ag$, where $a \in R$, g is primitive. Let R-UFD. Then every nonzero, nonunit is a product of irreducibles that are eithter in R or nonconstant, primitive, irreducible polynomials.

- **Theorem 16.16**: Let R be UFD, π is prime in $R[x]$. Then π is prime in $R[x]$.

  Proof. Suppose $\pi|fg$, fg nonconstant. Then $fg = ab(f'g')$ where $f'g'$ is primitive so $\pi|ab$, forcing $\pi|a$ or $\pi|b$. Then $\pi|f$ or $\pi|g$.

- **Lemma 16.18**: Let R be a UFD. F the field of fractoins of R. Let $f, g \in R[x]$, f primitive. Suppose $f|g$ in $F[x]$. Then $f|g$ in $R[x]$.

  Proof. Let $g = fh, h \in F[x], g, f$ as given. Then, $rh \in R[x]$ for some $r \in R$. Let $k = rh$, so we have $rg = fk$, where $r, g, f, k \in R[x]$ ($r \in R$). Let n be the number of the irreducible (hence prime) factors of r. If $n = 0$, r is a unit, and $g = fkr^{-1}, kr^{-1} \in R[x]$ showing $f|g$ in $R[x]$. If $n > 0$, let π be a prime factor of r. Then $\pi|fx$. Since π is prime in R, it is also prime in $R[x]$, so $\pi|f$ or $\pi|k$. Since f is primitive,we must have $\pi|k$, so $k = pik_1$, for some $k_1 \in R[x]$. We divide by π to obtain $r_1 g = fk_1$ where $r_1 \in R$ and has $n - 1$ prime factors. We repeat until we have no prime factors left. This gives $f|g$ in $R[x]$.

- **Example**: $x^3 - 1$ see if divisible by $x - 1$.

- **Lemma 16.19 (Guass's Lemma)**: Let R be a UFD with field of fractions F. Suppose $f \neq 0$, $f \in R[x]$, and $f = gh$ for $g, h \in F[x]$. Then there is an α and $\beta \in F$ with $g_0 = \alpha g$, $h_0 = \beta h$ where $g_0, h_0 \in R[x]$ and $f = g_0 h_0$.

  Proof. First we find an $a, b \in R$, so that $ag_0 = bg$, where g_0 is primitive in $R[x]$. Let $\alpha = \frac{b}{a}, \beta = \frac{a}{b}, \alpha, \beta = F$. We have $f = (\alpha g)(\beta h) = g_0(\beta h)$. By Lemma 16.18, we must have $g_0|f$ in $R[x]$. Therefore, $h_0 = \beta h \in R[x]$.

- **Example**: $(x^2 - x - 6) = (\frac{2}{3}x - 2)(\frac{3}{2}x + 3) = \frac{3}{2}(\frac{2}{3}x - 2)\frac{2}{3}(\frac{3}{2}x + 3) = (x - 3)(x + 2)$.

- **Theorem 16.12**: If R is a UFD, so is $R[x]$.

  Proof. Note that $R[x]$ is an integral domain, and every element factors into irreducibles (true for R, for polynomials factor until degrees are minimal.) We wish to show irreducibles are prime in $R[x]$, then 16.8c gives us unique factorization. Note: true for irreducibles in R, since primes of R are also primes of $R[x]$, so suppose $\deg(f) > 0$ and f is irreducible. Note f must be pirme, and cannot be factored into two polynomials of lesser degree. Suppose $f|kl$, where $k, l \in R[x]$. Consider f as a member of $F[x]$, where F is the field of fractions of R. Since $F[x]$ is a PID, f must be prime in $F[x]$ (note, not a unit, since $\deg(f) > 0$, also f is irreducibles in $F[x]$ since it can't be factored into two polynomials of smaller degree). From Lemma 16.19, so $f|k$ or $f|l$ in $F[x]$. By 16.18, $f|k$ or $f|l$ in $R[x]$. Therefore, f is prime. Note: If $f \in \mathbb{Z}[x]$ is nonconstant and primitive, then it's irreducible in $\mathbb{Z}[x]$ if and only if it's irreducible in $\mathbb{Q}[x]$.

- **Irreducible polynomials**: How do you find them? Degree 1, primitive $\Rightarrow$ irreducible. In $F[x]$, when is a degree 2 or 3 polynomial irreducible? If and only if the polynomial has a root in F. Higher degree? $x^4 + 2x^2 + 1$ in $\mathbb{Q}[x]$, no roots but $x^4 + 2x^2 + 1 = (x^2 + 1)^2$.

- **Theorem 16.21 (Eisenstein)**: Let R be a UFD, F field of fractions. Let $f \in R[x]$, $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Then f is irreducible in $F[x]$ if there is a prime π with

  1) $\pi \not| a_n$.
  2) $\pi | a_i$ for $0 \leq i \leq n$.
  3) $\pi^2 \not| a_0$.

- **Prime ideal**: a proper ideal I such that $a, b \in I$ implies a or $b \in I$. Note: if $a \in R$ is prime, then (a) is a prime ideal. $(2, x) = \{2a + xb\}$ is prime in $\mathbb{Z}[x]$, but not principal.
- **Lemma**: Let $I \subseteq R$ be an ideal, $I \neq R$. Then I is a prime ideal if and only if R/I is an integral domain.

  Proof.

  ($\Leftarrow$) Suppose this is an integral domain. Suppose $ab \in I$. We have $(a+I)(b+I) = ab+I = I$. Since R/I is an integral domain, $a + I = I$ or $b + I = I$. Therefore, $a \in I$ or $b \in I$. This shows I is prime.

  ($\Rightarrow$) Suppose that I is prime. If $(a + I)(b + I) = I$, then $ab \in I$, forcing $a \in I$ or $b \in I$. Then, $a + I = I$, $b + I = I$ implying R/I is an integral domain.
- **Addendum to Corollary 12.14**: Let $M \subseteq R$ be a proper ideal. Then M is maximal if and only if R/M is a field.

  Proof. By the correspondence theorem, ideals of R/M, corresponds to ideals of R containing M. By Corollary 12.12, R/M is a field if and only if its only ideals are $\{M\}$ and R/M. This occurs if and only if the only ideals of R containing M are R, M. This is equivalent to M being maximal.
- **Corollary**: Maximal ideals are prime.

  Proof. Let M be a maximal ideal. Then R/M is a field. Since fields are integral domains. R/M is an integral domain. So M is prime.
- **Example of a prime ideal that is not maximal**: (x) in $\mathbb{Z}[x]$, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, $(x) \leq (x, 2) \leq \mathbb{Z}[x]$.
- **Example**: In $\mathbb{Z}$, $6 = 2 \cdot 3 = (-2)(-3)$, $6 \in (2\mathbb{Z})(3\mathbb{Z})$, $30 \in (2)(3)(5)$. Find collections of prime ideals so that each nonzero, nonunit is in a unique product of some of these prime ideals.
- **Summary of commutative rings**:
  - ID, PID, Noetherian, UFD, Field, Field of fraction elements, 0, unit, prime, irreducible, zero divisor, primitive polynomial.
  - ID: prime $\Rightarrow$ irreducible.
  - Noetherian: nonunits factor into irreducibles.
  - UFD: irreducible $\Leftrightarrow$ prime.
  - PID: UFD, a irreducible $\Leftrightarrow$ a is prime $\Leftrightarrow$ (a) is maximal $\Leftrightarrow$ (a) is prime.
  - $F[x]$: is a PID (F a field).

8 Fields

- Characteristic of a field: smallest $n \in \mathbb{N}$ such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. Say it is characteristic 0 if no such n exists.
- **Theorem**: The characteristi of a field is either 0 or a prime.
- **Example**: $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.
- **Field growing recipe**: Take F_1 construct $F[x]$. Find irreducible polynomial $f(x)$ in $F[x]$. Construct quotient $F[x]/(f)$ - new field, contains original field as constants.
- **Example**: Start with $\mathbb{Z}_2$, $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$. Try $\mathbb{Z}_2/(x^2 + x + 1)$:

$$\begin{cases} (x^2 + x + 1) \\ 1 + (x^2 + x + 1) \\ x + (x^2 + x + 1) \\ 1 + x + (x^2 + x + 1) \end{cases}$$

- **Examples**:

  1) A field grows into a bigger field: $\mathbb{R} \subseteq \mathbb{C}$.

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

  where $i^2 = -1$. It is a field, e.g. $1 + 2i$, there is multiplicative inverse can be obtained by

  $$(1 + 2i)(1 - 2i) = 5 \Rightarrow (1 + 2i)\frac{1 - 2i}{5} = 1 \Rightarrow \frac{1}{5} - \frac{2}{5}i \in \mathbb{R}[i].$$

  Also, $\mathbb{C}$ can be regarded as an ordered pair (a, b).

2) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, which is a field. $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$. Again, $\mathbb{Q}[\sqrt{2}]$ is a 2-dimensional vector space.
3) $\mathbb{Q}[\sqrt[3]{5}] = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} : a, b, c \in \mathbb{Q}\}$. It is a field and 3-dimensional vector space.
4) $\mathbb{Q}[\pi] = \{a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n + \cdots, a_i \in \mathbb{Q}, i \in \mathbb{N}\}$. It is not a field. Note: $\mathbb{Q}[\pi] \cong \mathbb{Q}[x]$.

- **Defintion**: Dimension is denoted by $|E : F|$.
- **Definition**: If $F \subseteq E$, we say $\alpha \in E$ is algebraic over F if there is a polynomial in $F[x]$ which has α as a root.
- **Defintion**: If α is not algebraic, then it is called *trancendental*.
- If $F \subseteq E$, can construct a new field by taking $\alpha \in E/F$, α is algebraic over F and constructing $F[\alpha]$.
- Formal equivalent (not assuming E exists). Take field F, take polynomial f in $F[x]$ with f irreducible (degree at least 2). Let $E = F[x]/(f)$.
- Is E a field? $F[x]$ is a PID, so f is irreducible $\Leftrightarrow$ (f) is maximal (Lemma 16.9). $F[x]/(f)$ is a field since (f) is maximal.
- Does E contain F? Sort of. Treat constants $c + (f)$ where $c \in F$ as elements of F. Using this construction, $|E : F| = \deg((f))$, which is degree of field extension.
- **Example**: Find a field of order $16 = 2^4$. Need degree 4 irreducible polynomial over $\mathbb{Z}$. $x^4 + x^3 + x + 1$ does not work, when we plug $x = 1$, turns out $x = 1$ is the root of the polynomial. Hence it does not work. Take a look at $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Now we cannot factor $x^4 + x + 1$ into product of two polynomials of degree 2. Then construct
$$\mathbb{Z}_2[x]/(x^4 + x + 1) = \{a_0 + a_1x + a_2x^2 + a_3x^3 + x^4 + x + 1 : a_i \in \mathbb{Z}_2, i = 0, 1, 2, 3\}.$$
Change point of view, μ satisfying $\mu^4 + \mu + 1 = 0$, we have
$$\{a_0 + a_1\mu + a_2\mu^2 + a_3\mu^3 : a_i \in \mathbb{Z}_2, i = 0, 1, 2, 3\}.$$
- Starting from $\mathbb{Z}_p$, we can get a field of size of p^n for any $n \in \mathbb{N}$.