Algebra I

Spring 2018

Contents

1 Groups

Definition. A binary operation on a set X is a function $\star : X \times X \to X$. A set equipped with a binary operation is called a magma and is denoted $(X, \star)$.

Let $M = (X, \star)$ be a magma. We say $\star$ is associative if $a, b, c \in X$ then $(a \star b) \star c = a \star (b \star c)$. We say $\star$ is commutative if $a, b \in X$ then $a \star b = b \star a$.

Proposition 1.1. In any magma, if a two-sided identity exists, then it is unique.

Definition. A magma $(X, \star)$ is called

a) a semigroup if $\star$ is associative; or

b) a monoid if $\star$ is associative and has an identity.

Proposition 1.2. In a semigroup, all meaningful bracketings of $x_1 \star \cdots \star x_n$ are equivalent.

In a magma, $(X, \star)$, if $\alpha \in X$, then

$$\alpha^n = \begin{cases} \overbrace{\alpha \star \ldots \star \alpha}^{n}, & n > 0 \text{ (semigroup)} \\ e, & n = 0 \text{ (monoid)} \\ \underbrace{\alpha^{-1} \star \ldots \star \alpha^{-1}}_{|n|}, & n < 0 \text{ (group)} \end{cases}$$

In a monoid, we say $\alpha \in X$ has an inverse $\beta \in X$ if $\alpha \star \beta = e = \beta \star \alpha$. If α has an inverse, then it is a unit.

Proposition 1.3. In a monoid $(X, \star)$, if $\alpha \in X$ has an inverse, then its inverse is unique.

Definition (Group). A group $(G, \star)$ is a magma such that

a) $\star$ is associative;

b) there exists an identity $e \in G$; and

c) every $x \in G$ has an inverse, namely x^{-1}.

Examples. The following are all groups.

- $(\mathbb{Z}, +)$, integers under addition.
- $(\mathbb{R}^\times, \cdot)$, nonzero reals under multiplication.
- $GL_n(\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) : \det A \neq 0\}$, the general linear group.
- $(\Sigma(X) = \{f : X \xrightarrow{\text{bij}} X\}, \circ)$, bijective transformations under function composition.
- $\Sigma_n = (\Sigma(\{1, \ldots, n\}), \circ)$, symmetric group on n letters.
- Special linear group: $(SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}, \cdot)$
- Orthogonal group: $(O(n) = \{A \in \mathrm{Mat}_n(\mathbb{R}) : A^t A = I\}, \cdot)$

Proposition 1.4. Given a monoid $(M, \star)$, the set of units of M, denoted $U(M)$, forms a group under $\star$.

For a group G, given $a \in G$, we define $L_a : G \to G$ to be the left multiplication map, i.e. $L_a(x) = a \star x$. Define the right multiplication map R_a similarly. Both of these maps are always bijective.

Definition (Homomorphism). Suppose $(X, \star_1)$ and $(Y, \star_2)$ are magmas. A homomorphism is a function $f : X \to Y$ such that

$$f(\alpha \star_1 \beta) = f(\alpha) \star_2 f(\beta),$$

for all $\alpha, \beta \in X$. A bijective homomorphism is called an isomorphism.

1.1 Subgroups

Definition (Subgroup). Given $(G, \star)$ is a group, a subset $H \subset G$ is a subgroup if $(H, \star)$ is a group. This requires (a) H is closed under $\star$; (b) $e \in H$; and (c) $x \in H$ implies $x^{-1} \in H$.

Theorem 1.5

If $f : G_1 \to G_2$ is a homomorphism then

a) $f(e_1) = e_2$ where e_j is the identity in G_j, $j = 1, 2$;

b) $\forall x \in G_1$, $f(x^{-1}) = f(x)^{-1}$;

c) $\mathrm{Im}(f) \leq G_2$;

d) $\mathrm{Ker}(f) \leq G_1$.

Proposition 1.6. If $\{H_\alpha\}_{\alpha \in \mathcal{J}}$ is a collection of subgroups, then $\cap_{\alpha \in \mathcal{J}} H_\alpha$ is a subgroup.

Definition (Span). Let $S = \{x_j\}_{j \in \mathcal{J}} \subset G$, then the span of S is

$$\langle S \rangle = \{x_{j_1}^{\varepsilon_1} x_{j_2}^{\varepsilon_2} \dots x_{j_n}^{\varepsilon_n} : \varepsilon = \pm 1, n \in \mathbb{N}\}.$$

1.2 Cyclic Groups

Definition (Cyclic). A group is cyclic if there exists $\alpha \in G$ such that $G = \langle \alpha \rangle$.

Given a function $f : X \to X$, the forward orbit of $x \in X$ is $\{x, f(x), f(f(x)), \dots\}$. If f is bijective, the reverse orbit of x is $\{x, f^{-1}(x), f^{-1}(f^{-1}(x)), \dots\}$. In general, the orbit of x is the union of the forward and reverse orbits.

If f is a bijection, then either $f^{[n]}(x) \neq f^{[m]}(x)$ for any $m, n \in \mathbb{N}$; or for some $m \in \mathbb{N}$, the elements of the sequence $x, f(x), \dots, f^{[m-1]}(x)$ are distinct, but $f^{[m]}(x) = x$.

We say $\alpha \in G$ has infinite order if the forward order of e under L_α is an infinite set, that is $\langle \alpha \rangle = \{e, \alpha, \alpha^2, \dots\}$ has no duplicate elements. However, if $\{e, \alpha, \dots, \alpha^{m-1}\}$ are distinct but $\alpha^m = e$, then we say α has finite order m, denoted $|\alpha| = m$.

Theorem 1.7

If $\alpha \in G$ and

a) α has infinite order, then $\langle \alpha \rangle \cong (\mathbb{Z}, +)$.

b) $|\alpha| = m$, then $\langle \alpha \rangle \cong (\mathbb{Z}/m\mathbb{Z}, +)$.

Moreover, any cyclic group is isomorphic to one of $\mathbb{Z}$ or $\mathbb{Z}_n$.

Proposition 1.8.

a) Cyclic groups are abelian.

b) Subgroups of cyclic groups are cyclic.

Corollary. The only subgroups of $(\mathbb{Z}, +)$ are $\langle m \rangle$ for $m \in \mathbb{Z}$.

Theorem 1.9

Given $m, n \in (\mathbb{Z}, +)$, not both zero,

a) $\langle m, n \rangle = \{ms + nt : s, t \in \mathbb{Z}\} = \langle d \rangle$ for some $d \in \mathbb{Z}^+$.

b) $\exists s_0, t_0 \in \mathbb{Z}$, $\gcd(m, n) = s_0 m + t_0 n$ (Bezout's identity).

c) if $d = \gcd(m, n)$, then $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$

d) m, n relatively prime if and only if $\langle m, n \rangle = \mathbb{Z}$.

Corollary. If $\alpha \in \mathbb{Z}/m\mathbb{Z}$, then α has a multiplicative inverse if and only if $\gcd(\alpha, m) = 1$.

Lemma. A group homomorphism is injective if and only if its kernel is trivial.

Theorem 1.10

In $\mathbb{Z}/m\mathbb{Z}$, let $d, m \geq 1$,

a) if $d|m$ then $\langle d \rangle$ is cyclic of order $\frac{m}{d}$.

b) In general, $\langle \alpha \rangle = \langle \gcd(\alpha, m) \rangle$ is cyclic with order $\frac{m}{\gcd(\alpha, m)}$.

Definition. Given a group G with generating set S, the Cayley graph $\Gamma = \Gamma(G, S)$ is a colored digraph constructed as follows

- Each $g \in G$ is assigned a vertex.
- Each generator $s \in S$ is assigned a color c_s.
- For any $g \in G, s \in S$, the edge (g, gs), with color c_s, is in $E(\Gamma)$.

1.3 Symmetric Groups

Let $X = \{1, 2, \dots, n\}$. Recall that the symmetric group on n letters, Σ_n, is the set of all bijections $f : X \to X$. For example, in Σ_5, with array notation we can write

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

or equivalently,

$$\tau = (1245).$$

Proposition 1.11. Every permutation σ of a finite set is a product of disjoint cycles.

Proof. Let $B_1, \dots, B_r$ be the orbits of σ and let μ_i be the cycle defined by

$$\mu_i = \begin{cases} \sigma(x) & \text{for } x \in B_i \\ x & \text{otherwise} \end{cases}$$

Then $\sigma = \mu_1 \dots \mu_r$ and the μ_i are disjoint since the equivalence class orbits B_i are disjoint. ∎

Proposition 1.12. Let $\tau = (a_1 a_2 \dots a_k)$ and $\sigma = (b_1 b_2 \dots b_j)$ be distinct cycles. Then $|\tau| = k$ and $|\sigma\tau| = \operatorname{lcm}(k, j)$.

Definition. A transposition is a cycle composed of two elements.

Any permutation can be written be a product of transpositions. In particular, $(a_1 a_2 \dots a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_2)$.

Lemma. If $x \in \Sigma_n$ has t orbits in $\{1, \dots, n\}$ then $(ij)x$ has $t \pm 1$ orbits.

Proof. The proof breaks down into two cases, where i, j are in the same cycle or different cycles. In either case, it suffices to show the number of orbits changes by 1. ∎

Proposition 1.13. If $\sigma \in \Sigma_n$ and

$$\sigma = \tau_1 \tau_2 \dots \tau_r = \tau_1' \tau_2' \dots \tau_{r'}',$$

where τ_i are transpositions, then $r \equiv r' \bmod 2$.

Proof. Since any permutation can be expressed as a product of transpositions, we can equivalently generate the permutation by swapping rows in I_n. If C is a matrix obtained by a permutation σ of the rows of I_n, such that C can be obtained by both an odd and an even number of transpositions, then $\det C = 1$ and $\det C = -1$, a contradiction. ∎

Definition. Define A_n to be the set of all $\sigma \in \Sigma_n$ such that σ has even parity. We call A_n the alternating group.

Proposition 1.14. A_n is a subgroup of Σ_n and $|A_n| = \frac{n!}{2}$.

Theorem 1.15: Cayley

If G is a finite group, then G is isomorphic to a subgroup of some Σ_n.

Proof. Suppose $\phi : X \to X$ and $\theta : X \to \{1, \ldots, n\}$ are bijective. Define $\Psi : \Sigma(X) \to \Sigma_n$ by $\Psi(\phi) = \theta\phi\theta^{-1}$. It is easily verified that Ψ is a bijective homomorphism. Now, let G be a group with $|G| < \infty$ and define $\lambda : G \to \Sigma(G)$ by $\lambda(g) = L_g$. Again it is easily verified that λ is an injective homomorphism. Therefore, $\Psi\lambda : G \to \mathrm{Im}(\Psi\lambda)$ is an isomorphism. Moreover, $\mathrm{Im}(\Psi\lambda) \leq \Sigma_n$. ∎

1.4 Dihedral Groups

Given a simple graph (V, E), the automorphism group, $\mathrm{Aut}(V, E)$, is the set of all bijective function $f : V \to V$ that preserve adjacency. Note that this is a subgroup of $\Sigma(V) \cong \Sigma_{|V|}$.

Proposition 1.16. The order of D_n is $2n$ and $D_n = \{e, r, \ldots, r^n, s, rs, \ldots, r^{n-1}s\}$

Examples.

- For the complete graphs, K_n, we have $\mathrm{Aut}(K_n) = \Sigma_n$.
- For cycle graphs, $\mathrm{Aut}(C_n) = D_n = \{e, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$, where r is a rotation and s a reflection. Thus $|D_n| = 2n$.

1.5 Cosets & Lagrange

Definition (Coset). Given $H \leq G$, a left coset of H in G is a subset of the form $gH = \{gh : h \in H\}$. A right coset is defined similarly.

Lemma. If $H \leq G$ and $h \in H$, then $hH = H$.

Theorem 1.17

If $H \leq G$ and $g_1, g_2 \in G$, then

- $Hg_1 = Hg_2$ if and only if $g_1 = hg_2$ for some $h \in H$.
- $g_1H = g_2H$ if and only if $g_1 = g_2h$ for some $h \in H$.

Theorem 1.18

If $H \leq G$, then for any two left cosets g_1H and g_2H, either

a) $g_1H \cap g_2H = \varnothing$; or

b) $g_1H = g_2H$.

An analogous theorem applies for right cosets as well.

Corollary. If $H \leq G$, then the distinct left (right) cosets partition G.

Definition. Given $H \leq G$, define $(G : H)$ to be the index of H in G, that is the number of distinct left (right) cosets of H in G.

Lemma. If $H \leq G$ and $|G| < \infty$, then $|gH| = |H|$.

Theorem 1.19: Lagrange

If G is a finite group and $H \leq G$, then $|G| = |G : H||H|$. Thus $|H|$ divides $|G|$.

Warning. The converse of Lagrange's theorem, that for any divisor d of $|G|$ there exists a subgroup of order d, is not necessarily true.

Corollary. If $x \in G$ and $|G| < \infty$, then $|x|$ divides $|G|$.

1.6 Direct Products

Definition. Given $(G_1, \star_1), \ldots, (G_n, \star_n)$, the direct product $G_1 \times \ldots \times G_n$ under $\star$ is given by $(x_1, \ldots, x_n) \star (y_1, \ldots, y_n) = (x_1 \star_1 y_1, \ldots, x_n \star_n y_n)$. This product is also a group.

Theorem 1.20

If $(m, n) = 1$, then $(1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ has order mn, thus $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. Moreover, if $m = p_1^{\alpha_1} \ldots, p_t^{\alpha_t}$, for prime $p_1 < \ldots < p_t$, then $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_t^{\alpha_t}}$.

We say a finite group G is a p**-group** if $|G| = p^i$ for some prime p and some $i \in \mathbb{N}$.

Theorem 1.21: Structure Theorem 1

If A is any finite abelian group, then A is isomorphic to a finite product of cyclic p-groups. Furthermore, two finite abelian groups A, B are isomorphic if and only if the number of cyclic groups of type $\mathbb{Z}_{p^i}$ is the same for each p and $i \geq 1$.

1.7 Isometries

An (Euclidean) isometry is a function $f : \mathbb{R}^n \to \mathbb{R}^n$ such that

$$||f(x) - f(y)|| = ||x - y||,$$

for all $x, y \in \mathbb{R}^n$. Note that compositions of isometries are also isometries and that all isometries are injective.

Examples.

- The translation group: $\{T_b : b \in \mathbb{R}^n, T_b(x) = x + b\}$
- Orthogonal group: $\{L_A : A \in O(n)\}$
- Euclidean group: $E(n) = \{\Psi : \Psi(x) = Ax + b, A \in O(n), b \in \mathbb{R}^n\}$

Lemmas. Given orthonormal basis $u_1, \ldots, u_n$ of $\mathbb{R}^n$, there exists $A \in O(n)$ such that $Au_i = e_i$ for all $1 \leq i \leq n$, where e_i are the standard basis vectors.

A point $\vec{x} \in \mathbb{R}^n$ is uniquely determined by $||\vec{x}||$ and $||\vec{x} - e_i||$ for $1 \leq i \leq n$.

If $\Psi : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry such that $\Psi(0) = 0$ and $\Psi(e_i) = e_i$ for $1 \leq i \leq n$, then $\Psi = \text{id}$.

Theorem 1.22

The isometries of $\mathbb{R}^n$ are exactly $E(n)$. Moreover, the isometries of $\mathbb{R}^2$ are generated by translations, rotations, and reflections.

Every isometry of $\mathbb{R}^2$ is either a translation, reflection, rotation, or glide reflection (reflection + translation). Rotation about a point: $R_{c,\theta}(p) = c + R_{0,\theta}(p - c)$.

2 Quotient Groups

Definition (Normal). A subgroup N of a group G is normal if one of the following equivalent conditions hold.

a) $\forall g \in G$, $gN = Ng$.

b) $\forall g \in G$, $g^{-1}Ng = N$.

c) $\forall g \in G$, $g^{-1}Ng \subset N$.

d) $\forall n \in N, \forall g \in G$, $g^{-1}ng \in N$.

We write $N \trianglelefteq G$.

Proposition 2.1. Let $H \leq G$. Then left coset multiplication is well-defined by $(aH)(bH) = (ab)H$ if and only if H is a normal.

Proof. Given $xH = x'H$ and $yH = y'H$, we know that $x = x'h_1$ and $y = y'h_2$ for some $h_1, h_2 \in H$. Thus, $\forall x', y' \in G$, we have $xy = (x'h_1)(y'h_2) = (x'y')h$ if and only if

$$\begin{aligned} h_1 y' h_2 &= y'h \\ &\leftrightarrow h_1 y' = y'hh_2^{-1} = y'h' \\ &\leftrightarrow \forall y' \in G, Hy' \subseteq y'H. \end{aligned}$$

∎

Corollary. Let $H \trianglelefteq G$. Then the cosets of H forms a group G/H under the binary operation $(aH)(bH) = (ab)H$. This group is called the quotient group of G by H.

Proposition 2.2. Let $f : G \to G'$ be a homomorphism. Then there exists a homomorphism $\overline{f} : G/N \to G'$ such that $\overline{f}(\overline{x}) = f(x)$ for all $x \in G$ if and only if $N \subseteq \ker(f)$.

Proof. Suppose $\overline{f}$ exists. Then, for any $n \in N$, $f(n) = \overline{f}(\overline{n}) = \overline{f}(nN) = \overline{f}(eN) = \overline{f}(\overline{e}) = e$. Thus, $n \in \ker(f)$. Conversely, suppose $N \subseteq \ker(f)$. Then $xN = x'N$ if and only if $x = x'n$ for some $n \in N$. Thus $f(x) = f(x'n) = f(x')f(n) = f(x')$. Therefore, $\overline{f}$ is well-defined and for any $\overline{x}, \overline{y} \in G/N$, $\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$. ∎

$$
\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\
G/\ker(f) \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}
$$

Figure 1: Commutative diagram for theorem 2.3.

Theorem 2.3: First Isomorphism Theorem

Let $\varphi : G \to G'$ be a homomorphism. Then

a) $K = \ker(\varphi)$ is a normal subgroup of G.

b) there exists a homomorphism $\overline{\varphi} : G/K \to G'$ where $\overline{\varphi}(\overline{x}) = \varphi(x)$ for all $x \in G$.

c) $\mathrm{Im}(\varphi) = \mathrm{Im}(\overline{\varphi})$ is a subgroup of G'.

d) $G/ker(\varphi) \cong \mathrm{Im}(\varphi)$.

Proof. (a) Let $K = \ker(\varphi)$. Then, for any $g \in G$, $k \in K$, $\varphi(gkg^{-1}) = e$. Thus, $gkg^{-1} \in K$.

(d) It suffices to check that $\overline{\varphi}$ is one-to-one, but $\ker(\overline{\varphi}) = \overline{\ker(\varphi)} = \{\overline{e}\}$. ∎

2.1 FIT Applications

a) $\mathbb{R}/\mathbb{Z} \cong (S^1, \cdot)$ via $t \mapsto e^{2\pi i t}$.

b) $G/\{e\} \cong G$ by the identity homomorphism.

c) $G/G \cong \{e\}$ by the trivial homomorphism.

d) $G_1 \times G_2 / G_1 \times \{e\} \cong G_2$, via the projective homomorphism π_2.

e) $\mathrm{sgn} : \Sigma_n \to (\{\pm 1\}, \cdot)$, defined by

$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \in A_n \\ -1 & \text{otherwise} \end{cases}$$

is a homomorphism. Thus, $\ker(\mathrm{sgn}) = A_n$ is normal and $\sigma_n / A_n \cong (\{\pm 1\}, \cdot)$.

f) For any group G, $Z(G) \trianglelefteq G$. Note $PGL_n(\mathbb{R}) = GL_n(\mathbb{R})/Z(GL_n(\mathbb{R}))$ is called the projective linear group.

g) A **group commutator** is an element $[x, y] = xyx^{-1}y^{-1}$. Note that $[x, y] = e \leftrightarrow xy = yx$, $[x, y]^{-1} = [y, x]$, and for any homomorphism ϕ, $\phi([x, y]) = [\phi(x), \phi(y)]$. Define the **commutator subgroup** of a group G to be $[G, G] = \langle \{[x, y] : x, y \in G\} \rangle$.

Proposition 2.4. Then, we have that $[G, G] \trianglelefteq G$ and $G/[G, G]$ is abelian. We say $G/[G, G]$ is the **abelianization** of G, denoted G_{ab}.

Proposition 2.5. If $H \leq G$ and $|G : H| = 2$, then $H \trianglelefteq G$.

A **simple** group G is a group with no normal proper subgroups besides the trivial subgroup.

2.2 Classification of Finite Simple Groups

Every finite simple group is isomorphic to one of the following:

- Cyclic groups of prime order
- A_n, $n \geq 5$
- One of 16 families of Lie type
- One of 26 "sporadic" groups.

A **composition series** is a subnormal series $\{e\} = H_n \trianglelefteq H_{n-1} \trianglelefteq \ldots \trianglelefteq G = H_0$, such that each factor group H_i/H_{i-1} is simple. The factor groups are called **composition factors**. The Jordan-Hölder theorem states that any two composition series for a group G have isomorphic factors.

2.3 Group Action

A **group action** of a group G on a set X is given by $\rho : G \times X \to X$ subject to

a) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $g_1, g_2 \in G$, $x \in X$;

b) $e \cdot x = x$ for all $x \in X$

where $g \cdot x$ denotes $\rho(g, x)$.

Given $x_0 \in X$ and an action of G on X, we denote $\mathcal{O}_{x_0} = \{g \cdot x_0 : g \in G\}$ as the **orbit of** x_0 under the group action. The set of all $g \in G$ that fix x_0, $G_{x_0} = \{g \in G : g \cdot x = x\}$ is the **stabilizer (isotropy) subgroup of** x_0. A group action is **transitive** if X is non-empty and if for each pair $x, y \in X$ there exists a $g \in G$ such that $g \cdot x = y$.

Proposition 2.6. Given $x_0, x_1 \in X$ either $\mathcal{O}_{x_0} \cap \mathcal{O}_{x_1} = \varnothing$ or $\mathcal{O}_{x_0} = \mathcal{O}_{x_1}$.

Examples.

- $(g, xH) \mapsto gxH$ is a group action $G \times G/H \to G/H$.
- $(g_1, g_2) \mapsto g_1 g_2$ defines a group action $G \times G \to G$.
- $(g, x) \mapsto gxg^{-1}$ defines a group action $G \times X \to X$. The orbit $\mathcal{O}_{x_0}$ is called the **conjugacy class of** x_0. The isotropy subgroup G_{x_0} is the **centralizer of** x_0.

Proposition 2.7. (Orbit Stabilizer Theorem) Given G acting on X and $x_0 \in X$, there exists a bijection $\phi : G/G_{x_0} \to \mathcal{O}_{x_0}$. Thus $|\mathcal{O}_{x_0}| = |G : G_{x_0}| = |G|/|G_{x_0}|$, when G is finite.

Proof. Let $H = G_{x_0}$. Define ϕ by $\phi(gH) = g \cdot x_0$. Show ϕ is a well-defined bijection. ∎

Define X^G to be the set of all $x \in X$ that are fixed by every element of G, or equivalently, the set of $x \in X$ with orbit size one. Similarly, define X^g to be the set of all $x \in X$ fixed by $g \in G$. Note that $X^G = \cap_{g \in G} X^g = \cap_{x \in X} \mathsf{Stab}(x)$.

A corollary to proposition 2.7 is that

$$|X| = \sum_{\text{distinct } \mathcal{O}_x} |\mathcal{O}_x| = |G| \sum_{\substack{\text{distinct} \\ \text{stabilizers}}} \frac{1}{|G_x|}$$

Thus
$$|X| = |X^G| + |G| \sum_{\substack{\text{distinct } G_x \\ |\mathcal{O}_x|>1}} \frac{1}{|G_x|}.$$
In the particular case where G is a p-group we have
$$|X| \equiv |X^G| \pmod{p}.$$

Corollary. If $|G| = p^2$ then G is abelian and $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Corollary. If G is a p-group then $|G| \cong |Z(G)| \bmod p$. Thus, if G is non-trivial, then $p \big| |Z(G)|$, so $Z(G)$ is non-trivial.

Theorem 2.8: Cauchy

If p is prime and G is a finite group such that $p \big| |G|$, then G contains an element of order p.

Proof. Let $X = \{(g_1, \dots, g_p) : g_i \in G, g_1 \dots g_p = e\}$. Then $|X| = |G|^{p-1} \equiv 0 \bmod p$. Define $T : X \to X$ by
$$T(g_1, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1).$$
(Verify T indeed maps onto X). Then $\langle T \rangle$ is a cyclic p-group. Let $\langle T \rangle$ act on X, then $|X| \equiv |X^{\langle T \rangle}| \equiv 0 \bmod p$. However, $X^{\langle T \rangle}$ is precisely the set of all p-tuples $(x, \dots, x)$ satisfying $x^p = e$. Since $e^p = e$ and $p \geq 2$, we have existence. ∎

2.4 Burnside's Formula

Given G acting on X with $|X|, |G| < \infty$. Let r be the number of orbits in X under G, then
$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. Consider the set of all pairs $(g, x) \in G \times X$ such that $gx = x$ and let N be the number of such pairs. Then for some $g \in G$, $|X^g|$ is the number of x fixed by g, so
$$N = \sum_{g \in G} |X^g| \tag{2.1}$$

On the other hand, for some $x \in X$, $|G_x|$ is the number of $g \in G$ that fix x, so
$$N = \sum_{x \in X} |G_x|.$$
Recall that $|xG| = |G : G_x| = |G|/|G_x|$. Substituting we have
$$N = \sum_{x \in X} \frac{|G|}{|xG|}, \tag{2.2}$$
but since $1/|xG|$ is fixed for all x in the same orbit, for any orbit, $\sum_{x \in \mathcal{O}} \frac{1}{|xG|} = 1$. In other words, $\sum_{x \in X} \frac{1}{|xG|} = r$. By equating (2.1) with (2.2), we obtain the desired result. ∎

Example. Suppose we color the edges of a 3-gon from a set of 4 colors. Let S be the set of all possible colors (we assume that the vertices of the 3-gon are labeled). Thus $|S| = 4^3$. The number of distinguishable colorings is the number of orbits of S under D_3. There are 16 colorings which are fixed for each nontrivial reflection. There a 4 colorings which are fixed for each nontrivial rotation. Thus

$$\#\text{ orbits} = \frac{1}{6}(64 + 16 + 16 + 16 + 4 + 4) = 20.$$

3 Sylow Theory

Let G be a group and S the set of subgroups of G. Suppose G acts on S via conjugation. We denote the isotropy subgroup of H under this action by $N_G(H)$, the **normalizer** of H in G. Note that $H \trianglelefteq N_G(H) \leq G$, since by any element of H will fix H under conjugation, so H is a normal subgroup of its normalizer. Therefore $N_G(H)$ is well-defined and

$$|G : H| = |G : N_G(H)||N_G(H) : H|.$$

Thus $|G : N_G(H)|$ divides $|G : H|$.

Lemma. If P is a p-subgroup of a finite group G, then

$$|G : P| = |N_G(P) : P| \bmod p.$$

Proof. Consider P acting on G/P via $p(xP) = (px)P$. Then $p(xP) = xP \leftrightarrow x^{-1}px \in P$. Therefore, $xP \in (G/P)^P \leftrightarrow x \in N_G(P)$. Hence $(G/P)^P = N_G(P)/P$. Therefore since $|(G/P)^P| \equiv |G/P| \bmod p$, we're done. ∎

Theorem 3.1: Sylow I

Let G be a finite group with $|G| = p^\alpha m$ such that $\gcd(m, p) = 1$ for some prime p. Then there exists

$$e \trianglelefteq P_1 \trianglelefteq \ldots \trianglelefteq P_\alpha \leq G,$$

such that $|P_i| = p^i$ for all $1 \leq i \leq \alpha$.

Proof. We proceed by induction on i. For $i = 0$, it's trivial. Assume we have

$$e \trianglelefteq P_1 \trianglelefteq \ldots \trianglelefteq P_j \leq G,$$

such that $|P_i| = p^i$ for all $1 \leq i \leq j < \alpha$. Then $|G : P_j| = p^{\alpha - j}m \equiv 0 \bmod p$. Thus $|N_G(P_j)/P_j| \equiv |N_G(P_j) : P_j| \equiv 0 \bmod p$, which implies $|N_G(P_j)/P_j|$ is a nonzero multiple of p. ∎

Definition. A **Sylow p-subgroup** P of a group G is a maximal p-subgroup of G. Define $\mathrm{Syl}_p(G)$ to be the set of all Sylow p-subgroups of G and $n_p(G)$ the number of Sylow p-subgroups of G.

Theorem 3.2: Sylow II

Given G as in 3.1, any two Sylow p-subgroups of G are conjugate and thus isomorphic.

Theorem 3.3: Sylow III

Given G as in 3.1, $n_p(G) = |G : N_G(P)| \equiv 1 \bmod p$.

Theorem 3.4: Sylow IV

Given G as in 3.1, any p-subgroup of G is a subgroup of a Sylow p-subgroup of G.

3.1 Applications

Proposition 3.5. Let $|G| = pq$ for distinct primes $p > q$. Then there exists a normal subgroup $N \trianglelefteq G$ such that $|N| = p$. Thus G isn't simple.

Proof. We have $n_p(G) \mid q$ and $n_p(G) \equiv 1 \bmod p$. Thus $n_p(G) = 1$, so there is only one Sylow p-subgroup, say P. By Sylow II, P is normal. ∎

Lemma. Given $N_1, N_2 \trianglelefteq G$ with $N_1 N_2 = G$ and $N_1 \cap N_2 = \{e\}$, then $G \cong N_1 \times N_2$.

Proof. We'll show that for any $x \in N_1, y \in N_2$ we have $xy = yx$. Consider $(xyx^{-1})y^{-1} = x(yx^{-1}y^{-1})$ which is clearly in the intersection of N_1 and N_2. Thus, $xyx^{-1}y^{-1} = e$, i.e. $xy = yx$. Now define $\theta : N_1 \times N_2 \to G$ such that $\theta(x, y) = xy$. Then θ is the desired isomorphism. ∎

Proposition 3.6. If $|G| = pq$ for distinct primes $p > q$ and $p \not\equiv 1 \bmod q$, then $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

Proof. As in prop. 3.5. $n_p(G) = 1$ and by the hypothesis that $p \not\equiv 1 \bmod q$ we have $n_q(G) = 1$. Denote the Sylow p and q-subgroups by P and Q, respectively. By Lagrange, $x \in P \cap Q$ then $|x|$ divides p and q. Thus $x = e$. Recall that $|PQ| = |P||Q|/|P \cap Q| = |G|$, so $PQ = G$. By the lemma, we're done. ∎

Proposition 3.7. Let $|G| = p^a q$ for distinct primes $p > q$. Then G has a normal Sylow p-subgroup so G is not simple.

Proposition 3.8. Let $G = pqr$ for distinct primes $p < q < r$. Then either G has a normal Sylow r-subgroup of G has a normal Sylow q-subgroup. Thus G isn't simple.

Proof. $n_r(G) \mid pq$ and $n_r(G) \equiv 1 \pmod r$, thus either $n_r(G) = 1$, in which case we're done, or $n_r(G) = pq$. WLOG we have $n_r(G) = pq$. If $R \in \mathrm{Syl}_r(G)$ then R is cyclic. Thus R has $r - 1$ elements of order r. If $R' \neq R$ is some other Sylow r-subgroup, then $R \cap R' = \{e\}$. Thus the number of elements of order r in G is $pq(r - 1)$. In particular, the number of elements of order not equal to r is pq. Then $n_q(G) = 1$, r, or pr. So WLOG $n_q(G) \geq r$. Thus the number of elements of order q is at least $r(q - 1)$. Therefore, $r(q - 1) < pq$, a contradiction. ∎

It is a well-known result that if G is a non-abelian simple group then $|G| \geq 60$. In particular A_5 is the smallest such group.

4 Rings & Fields

Definition. A ring $(R, +, \cdot)$ is a set R equipped with two binary operations, "addition" $(+)$ and "multiplication" $(\cdot)$ such that:

(1) $(R, +)$ is an abelian group with identity 0;

(2) $(R, \cdot)$ is a monoid with identity 1; and

(3) for any $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

We denote the additive inverse of $x \in R$ by $-x$ and the multiplicative inverse x^{-1} (if it exists). We say a ring is commutative if and only if $\cdot$ is commutative. The set of units of the ring R is the set of units of the monoid $(R, \cdot)$.

Proposition 4.1. For any $x, y \in R$

a) $0 \cdot x = 0 = x \cdot 0$

b) $x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$

c) $(-x) \cdot (-y) = x \cdot y$.

It follows that for any nontrivial ring R we have $0 \neq 1$.

A ring R such that $\text{Units}(R) = R \backslash \{0\}$ is a **division ring**. A commutative division ring is called a **field**. A subset S of a ring R is a **subring** if $(S, +, \cdot)$ is also a ring (S must be closed under the binary operations). A subset S of a field F is a **subfield** if S is a subring of F such that for any $x \neq 0$ in S, then $x^{-1} \in S$, that is S is also a field.

Definition. Given rings R_1, R_2, a ring homomorphism is a function $f : R_1 \to R_2$ such that for all $x, y \in R_1$,

a) $f(x + y) = f(x) + f(y)$

b) $f(xy) = f(x)f(y)$

c) $f(1) = 1$.

In particular, if f is bijective, then f is a ring isomorphism.

The **kernel** of the ring homomorphism $f : R_1 \to R_2$ is $\ker(f) = \{x \in R : f(x) = 0\}$. Thus, by group theory, f is injective if and only if the kernel of f is trivial.

A **pair of zero divisors** in a ring is a pair of nonzero elements $x, y \in R$ such that $xy = 0$. We say x and y are individually **zero divisors**. An **integral domain** is a commutative ring with no zero divisors.

Proposition 4.2. If R is an integral domain and $a, x, y \in R$, then $ax = ay$ implies $x = y$ when $a \neq 0$.

Proof. Assume $a \neq 0$. We have $ax = ay$, so $a(x - y) = 0$. Since R is an ID, it has no zero divisors, hence $x - y = 0$. ∎

Proposition 4.3. If R is an ID, then $R[X]$ is an ID.

Proposition 4.4. If R is a finite ID, then R is a field.

Given a ring $(R, +, \cdot)$, if the order of 1 in $(R, +)$ is infinite, we say R has **characteristic 0**. Otherwise, if the order of 1 is m, then we say R has **characteristic** m.

Note that if R is an ID, either R has characteristic 0 or R has prime characteristic.

4.1 Euler's Theorem

The Euler phi function $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Note $\phi(p^a) = (p-1)p^{a-1}$ for prime p.

Proposition 4.5. If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. This follows from the fact that $\rho : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ given by $\rho(\alpha) = (\alpha, \alpha)$ is a ring homomorphism and the number of units of $R \times S$ is the number of units of R times that of S. ∎

Corollary. If $n = p_1^{a_1} \dots p_k^{a_k}$, then $\phi(n) = \phi(p_1^{a_1}) \dots \phi(p_k^{a_k})$.

Euler's Theorem. For any $a \in \mathbb{Z}$, we have $a^{\phi(m)} \equiv 1 \bmod m$. Note that FLT is a special case of Euler's theorem, where m is prime.

4.2 Field of Quotients

Theorem 4.6

If R is a subring of a field, then R is an ID. Moreover, if R is an ID, then there exists a field F such that R is a subring of F.

Proof. The first way is obvious. So let R be an ID. We'll construct the 'field of fractions' as follows. Define $pre(F) = \{(r, s) \in R \times S \backslash \{0\}\}$. Define $\sim$ on $pre(F)$ by $(r, s) \sim (r', s')$ if and only if $rs' = sr'$. Then $\sim$ is an equivalence relation. It follows that $F = pre(F)/\sim$ is a field. Furthermore, the injection $\theta : R \to F$ by $\theta(r) = (r, 1)$ is a ring homomorphism, so 'R is in F'. ∎

4.3 Rings of Polynomials

Let R be a commutative ring and $R[x]$ the ring of polynomials with coefficients in R. Given $p \in R$ define the evaluation map $\mathsf{ev}_p : R[X] \to R$ by $\mathsf{ev}_p(f(x)) = f(p)$. Note ev_p is a ring homomorphism.

Definition. Given $f(x) \in R[x]$ and $p \in R$, p is a root of $f(x)$ if and only if $f(p) = 0$. Equivalently, $\mathsf{ev}_p(f(x)) = 0$ or $f(x) \in \ker \mathsf{ev}_p$.

Proposition 4.7. Let F be a field. Given $p(x) \in F[x]$ and $q(x) \in F[x]\backslash\{0\}$ there exists polynomials $s(x)$ and $r(x)$ such that

$$p(x) = s(x)q(x) + r(x) \text{ in } F[x],$$

where $r(x)$ has degree 0 or degree less than $p(x)$.

Proof. The claim is trivial when $p(x) = 0$. So WLOG $p(x) \not\equiv 0$. If $\deg(p) < \deg(q)$, there is nothing to prove. So WLOG assume $\deg(p) \geq \deg(q)$. Say $p(x) = a_0 + \dots a_k x^k$ and $q(x) = b_0 + \dots + b_l x^l$

where $k \geq l$, $a_k \neq 0$, and $b_l \neq 0$. We'll induct on k. The base case is when $k < l$. Consider $n(x) = p(x) - \frac{a_k}{b_l}x^{k-1}q(x)$. We have $\deg(n) < k$. By the inductive hypothesis, we have $n(x) = \hat{s}(x)q(x) + r(x)$ for suitable $r(x)$. Hence $p(x) = s(x)q(x) + r(x)$, for $s(x) = \hat{s}(x) + \frac{a_k}{b_l}x^{k-l}q(x)$ ∎

4.4 Factorization

Proposition 4.8. If F is a field and $p(x) \neq 0 \in F[x]$, then $\alpha \in F$ is a root of p if and only if $p(x) = (x - \alpha)q(x)$ for $q(x) \in F[x]$.

Corollary. If F is a field and $p(x) \neq 0 \in F[x]$ with $\deg(p(x)) = d$, then p has at most d distinct roots in F. Similarly, if R is an ID and $p(x) \neq 0 \in R[x]$ has $\deg(p(x)) = d$, then p has at most d distinct roots in R.

Proposition 4.9. Let F be a field and let $F^\times$ denote the multiplicative group of units of F. If G is a subgroup of $F^\times$ then G is cyclic.

Corollary. In the field $\mathbb{Z}_p$, there exists at least one primitive generator α such that $\{1, \alpha, \ldots, \alpha^{p-2}\} = \{1, \ldots, p-1\}$.

Corollary. Let R be an ID and $R^\times$ the multiplicative group of units of R. If G is a finite subgroup of $R^\times$, then G is cyclic.

Let R be an ID and let $x \neq 0$ be in R. A factorization $x = ab$ can be **proper** or **improper**. The later being the case where either a or b is a unit, the former where neither is a unit. If x is a non-unit, then x is **reducible** if it has a proper factorization. Otherwise, we say x is **irreducible**. If $x, y \in R$ such that $x = uy$ for a unit $u \in R$, then we say x and y are **associates**. Note the associate relation is an equivalence relation, which partitions R into **associate classes**.

- Over any field, all linear polynomials are irreducible.
- A quadratic and cubic polynomial is irreducible in $F[x]$ if and only if it doesn't have a root in F.
- Let F be a field of $\text{char}(F) \neq 2$. Then $ax^2 + bx + c$, $a \neq 0$, has a root α in F if and only if $\Delta = b^2 - 4ac$ is a square in F. That is, there exists $\beta \in F$, such that $\beta^2 = \Delta$. When this happens
$$\alpha = \frac{-b \pm \beta}{2a}.$$

Lemma (Gauss). Let $p(x)$ be a non-constant polynomial with integer coefficients. If $p(x)$ is irreducible over $\mathbb{Z}[x]$, then $p(x)$ is irreducible over $\mathbb{Q}[x]$.

Eisenstein's Criterion. Let $n \geq 1$ and $q(x) = a_0 + \ldots + a_n x^n$ with $a_i \in \mathbb{Z}$ and $a_n \neq 0$. If p is a prime such that $p \mid a_j$ for $0 \leq j < n$, $p \nmid a_n$ and $p^2 \nmid a_0$, then q is irreducible over the rationals.

Proof. Suppose $Q(x)$ satisfies the above criterion but is reducible over $\mathbb{Q}[x]$. By Gauss' lemma, Q is reducible in $\mathbb{Z}[x]$, so it can be written $Q = GH$ for two non-constant polynomials G and H. Reducing $Q = GH$ modulo p, all but the leading term of Q vanishes, by hypothesis. But then, necessarily, all but the leading terms of G and H vanish. In particular, the constant terms of G and H vanish, so they are divisible by p. Hence p^2 divides the constant term of Q, a contradiction. ∎

Example. (Cyclotomic polynomials) Consider $\Phi_p(x) = \frac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$. By Eisenstein, $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}[x]$, thus $\Phi(x)$ is irreducible over $\mathbb{Q}[x]$.

The p-adic valuation of an integer n, denoted $\nu_p(n)$, is the largest power of p that divides n. For example, Legendre's formula is $\nu_p(n!) = \sum_{k\geq 1} \lfloor \frac{n!}{p^k} \rfloor$.

Definition (UFD). A ring R is a unique factorization domain (UFD) if

a) R is an ID;

b) for any nonzero $x \in R$, $\exists u, p_1, \ldots, p_j$ where u is a unit, p_i are irreducibles, and $p_i \not\sim p_j$ whenever $i \neq j$, such that $x = up_1^{\ell_1} \ldots p_k^{\ell_k}$ for $\ell_1, \ldots, \ell_k \in \mathbb{Z}_{\geq 0}$;

c) if $up_1^{\ell_1} \ldots p_k^{\ell_k}$ and $vq_1^{m_1} \ldots q_s^{m_s}$ are two factorizations of x (as in (b)), then $k = s$ and $\exists \sigma \in \Sigma_S$ such that $p_i \sim q_{\sigma(i)}$ and $\ell_i = m_{\sigma(i)}$ for all $1 \leq i \leq s$.

Definition (ED). A ring R is a Euclidean Domain (ED) if

a) R is an ID;

b) $\exists f : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ called the Euclidean function satisfying $f(a) \leq f(ab)$ for all $a, b \in R\backslash\{0\}$;

c) (Euclidean algorithm) if nonzero $\alpha, \beta \in R$ then $\alpha = q\beta + r$ where $r = 0$ or $f(r) \leq f(\beta)$.

Examples.

- $\mathbb{Z}$ with $f(n) = |n|$ is a ED.
- For a field F, $F[x]$ with $f(p(x)) = \deg(p(x))$ is a ED.
- (Gaussian integers) $\mathbb{Z}[i]$ with $f(a+bi) = a^2 + b^2$ is a ED. Note for $a + bi, c + di \in \mathbb{Z}[i]$, we have
$$a + bi = (c+di)(\lambda + \mu i) + \underbrace{(c+di)((\gamma + \delta i) - (\lambda + \mu i))}_{r}$$
where $\gamma + \delta i = \frac{a+bi}{c+di}$ and $\lambda + \mu i \in \mathbb{Z}[i]$ minimizes $\Delta = \left\|(\lambda + \mu i) - (\gamma + \delta i)\right\|^2$. We have $\Delta \leq \frac{1}{2}$ so $\|r\|^2 \leq \frac{1}{2}\|c + di\|^2$.

Proposition 4.10. Any ED is a UFD.

Lemma. Let R be an ED with Euclidean function $f : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$. Then (a) $f(1) = \min_{x \in R\backslash\{0\}} f(x)$ (b) x is a unit if and only if $f(x) = f(1)$ (c) $f(a) = f(ab)$ for some $a \neq 0$ if and only if b is a unit and (d) if α, β are associate, then $f(\alpha) = f(\beta)$.

Proof. (a) Set $a = 1$ if $f(a) \leq f(ab)$.

(b) $f(x) \leq f(xx^{-1}) = f(1)$, so $f(x) = f(x)$ by a. Conversely, if $f(x) = f(1)$, then $1 = qx + r$ where $r = 0$ or $f(r) < f(x) = f(1)$. Thus $r = 0$ and $qx = 1$.

(c) For the reverse direction, $f(a) \leq f(ab) \leq f((ab)b^{-1}) = f(a)$. Conversely, we have $a = (ab)c + r$ for $r = 0$ or $f(r) < f(ab) = f(a)$. If $r \neq 0$, then $r = a(1 - bc)$ so $f(a) \leq f(a(1 - bc)) = f(r)$, contradiction. (d) is a special case of (c). ∎

Proposition 4.11. Let R is an ED and $\alpha \neq 0$ in R. If $\alpha = x_1 \ldots x_n$ where $n > f(\alpha)$ then at least one x_j is a unit.

Proof. Suppose $\alpha = x_1 \dots x_n$ where x_j is not a unit. Then $f(\alpha) = f(x_1(x_2 \dots x_n)) > f(x_2 \dots x_n) > \dots f(x_n) > f(1) \geq 0$, i.e. $f(\alpha) \geq n$. ∎

Corollary. (Existence of factorizations in EDs) If R is a ED and $x \neq 0$ in R, then x has a factorization as in the definition of UFD.

Definition (Prime). Let R be an ID, a nonzero, non-unit $p \in R$ is prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Proposition 4.12. Primes are irreducible.

Proposition 4.13. In any ID, if $up_1^{\ell_1} \dots p_k^{\ell_k} = vq_1^{m_1} \dots q_s^{m_s}$, where the p_j, q_i are primes, $p_i \not\sim p_j$ and $q_i \not\sim q_j$. Then $k = s$ and $\exists \sigma \in \Sigma_S$ such that $p_i \sim q_{\sigma(i)}$ and $\ell_i = m_{\sigma(i)}$ for all $1 \leq i \leq s$.

Proof. Induction on $n = \min(k, s)$. ∎

4.4.1 Ideals

Definition (Ideal). A subset I of a ring R is a left ideal if I is an additive subgroup of $(R, +)$ and $ra \in I$ for any $a \in I$ and $r \in R$. Right ideals and two-sided ideals are defined similarly. For simplicity, we'll refer to a two-sided ideal as simply an ideal.

Examples.

- Any ring R is an ideal of itself (called the *improper ideal*). The *trivial ideal* $\{0\}$ is always an ideal of R.
- There are left ideals that are not two-sided, e.g. the set of all matrices in $\mathrm{Mat}_n \mathbb{C}$ with a 0 first column is a left sided ideal only.
- Let $R = \mathrm{Mat}_n(\mathbb{C})$. Then R is a *simple ring*: that is, it has no proper nontrivial ideals. *Pf.* Let J be an ideal. If nonzero $A \in J$ with $a_{ij} \neq 0$, then $(\frac{1}{a_{ij}} E_{ij}) A (E_{jk}) = E_{lk} \in J$. Since J is additive, we have $J = R$.
- If R is commutative and $a \in R$, then $(a) = \{ra : r \in R\}$ is the *principal ideal generated by* a. More generally, $(a_1, \dots, a_n) = \{a_1 r_1 + \dots + a_n r_n : r_1, \dots, r_n \in R\}$.
- If J contains a unit of R, then $J = R$. Hence proper ideals do not contain units.
- If R is commutative, then R is simple if and only if R is a field.
- (Artin-Wedderburn). If R is a finite ring, then R is simple if and only if it is isomorphic to $\mathrm{Mat}_n(\mathbb{F})$.
- In a commutative ring, there can be non-principal ideals, e.g. the subset $J \subset R[x, y]$ consisting of polynomial with constant term 0.

Proposition 4.14. Let R be an ID and $\alpha, \beta \in R$. Then $(\alpha) = (0)$ if and only if $\alpha = 0$, $(\alpha) \subset (\beta)$ if and only if $\beta \mid \alpha$, $(\alpha) = (\beta)$ if and only if $\alpha \sim \beta$, $(\alpha) = R$ if and only if α is a unit, and α is irreducible if and only if (α) is a maximal proper principal ideal.

Definition (PID). A principal ideal domain R is an integral domain, all of whose ideals are principal.

Proposition 4.15. Any ED is a PID.

Proof. Consider $\alpha = \arg\min_{\beta \in J \setminus \{0\}} f(\beta)$. For any $y \in J$, if $y = q\alpha + r$, then $r = 0$ or $f(r) < f(\alpha)$. Thus $r = 0$ and $y \in (\alpha)$. ∎

Corollary. In a ED, $(\alpha, \beta) = (d)$ where d is called the *greatest common divisor of α and β.*

4.5 Quotient Rings

Given a ring R and a proper ideal I, the quotient ring $(R/I, +)$ is well-defined with $(r_1+I)(r_2+I) = (r_1 r_2) + I$.

Definition. An ideal M of R is called a **maximal ideal** if $M \neq R$ and for any ideal I in R, if $M \subset I$ then either $I = M$ or $I = R$.

For example, in a PID, α is an irreducible element if and only if (α) is a maximal ideal.

Definition. An ideal P of R is called a **prime ideal** of R is $I \neq R$ and $ab \in P$ if and only if either $a \in P$ or $b \in P$.

For example, in any commutative ring R, the ideal generated by 0 is prime if and only if R is an integral domain. Furthermore, if R is an integral domain, then $\alpha \in R$ is prime if and only if (α) is a nonzero prime ideal.

Theorem 4.16

Let R be a commutative ring and I a proper ideal.

a) R/I is a field if and only if I is a maximal ideal.

b) R/I is an integral domain if and only if I is a prime ideal.

As a corollary to theorem 4.16, we see that if an ideal I of a commutative ring R is a maximal ideal, then I is prime, since every field is an integral domain. Moreover, in a PID, irreducibility implies primality.