Algebra Preliminary Exam Notes

This is a list of most of the definitions, theorems, and propositions contained within *Abstract Algebra* 3^{rd} *edition* by Dummit and Foote as well as some extra useful ones. References made in red in this series of notes refer to the actual number of the theorem in the book.

Contents

1. Introduction to Groups

Theorem 1.1. Let $(G, \cdot)$ be a group, $H \subseteq G$. Then $(H, \cdot)$ is a subgroup of G if

1. $H \neq \varnothing$.
2. For all $a, b \in H$, $ab^{-1} \in H$.

Definition 1.2. Let $g \in G$ a group, then g^{-1} is the unique element of G such that $gg^{-1} = g^{-1}g = id$

Definition 1.3. A ***group action*** of a group G on a set A is a map, $G \times A$ to A satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G$ and $a \in A$.
2. $id_G \cdot a = a$ for all $a \in A$.

2. Subgroups

Definition 2.1. Let $A \subseteq G$, $A \neq \varnothing$. Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the ***centralizer*** of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A. When $A = G$ this set is denoted by $Z(G)$ and is called the ***center*** of G.

Note: $Z(G) \leq C_G(A)$ for all $A \subseteq G$.

Definition 2.2. Let $A \subseteq G$, $A \neq \varnothing$. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. We define the ***normalizer*** of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Definition 2.3. Let G be a group acting on a set S. The ***stabilizer*** G_s for some fixed $s \in S$ is the set

$$G_s = \{g \in G \mid g \cdot s = s\}.$$

Proposition 2.4. Let A be some set and G be a group. Then $C_G(A) \leq N_G(A)$.

Proof. $C_G(A)$ is the kernel of $N_G(A)$ acting on A under the conjugation map $a \mapsto gag^{-1}$. ♣

Proposition 2.5. Let G be a group and $S \subseteq G$, $s \neq \varnothing$. Then $N_G(S) \leq G$.

Proof. Let G be a group and $S \subseteq G$. We know that $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$. If we take $a, b \in N_G(S)$ we have that

$$abSb^{-1}a^{-1} = aSa^{-1} = S$$

so $ab \in N_G(S)$. Similarly we have that for $a \in N_G(S)$

$$a^{-1}Sa = a^{-1}(aSa^{-1})a = S$$

so $a^{-1} \in N_G(S)$ and we have that $N_G(S) \leq G$. ♣

Theorem 2.6. There is only one cyclic group of each order.

Proposition 2.7. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z}^{\times}$.

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

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

Definition 2.8. Let $A \subseteq G$ and define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

This is called the ***subgroup of G generated by A*** and is simply the intersection of all the subgroups containing the set A.

Zorn's Lemma. If A is a nonempty partially ordered set in which every chain has an upper bound then A has a maximal element.

3. Quotient Groups and Homomorphisms

Proposition 3.1. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

1. $\varphi(id_G) = id_H$
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$
3. $\varphi(g^n) = \varphi(g)^n$
4. $\ker(\varphi)$ is a subgroup of G
5. $\operatorname{im}(\varphi)$ is a subgroup of H

Proposition 3.2. Let G be a group and let N be a subgroup of G

1. The operation on the set of left cosets of N in G described by

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

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

2. If the above operation is well defined then it makes the set of left cosets of N in G into a group. In particular the identity of this group is the coset $id_G N$and the inverse of gN is $g^{-1}N$.

Definition 3.3. The element gng^{-1} is called the conjugate of $n \in N$ by g. The set gNg^{-1} is also called the conjugate of N by g. The element g is said to ***normalize*** N if $gNg^{-1} = N$. A subgroup N of G is a ***normal subgroup*** if every $g \in G$ normalizes N. We will write this as $N \trianglelefteq G$.

Theorem 3.4. Let N be a subgroup of G. The following are equivalent.

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $gN = Ng \quad \forall g \in G$
4. The operation on left cosets of N in G described by Proposition 3.2 makes the set of left cosets into a group
5. $gNg^{-1} \subseteq N$ for all $g \in G$.

Lagrange's Theorem. If G is a finite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.

Cauchy's Theorem. If G s a finite group and p is a prime dividing $|G|$ then G has an element of order p.

Definition 3.5. (Dedekind and Hamiltonian Groups) For any group G, if all the subgroups of G are normal then G is called a *Dedekind* group. If G is non-abelian then G is called a *Hamiltonian* group.

Theorem 3.6. If G is a finite group of order $p^\alpha m$, where p is a prime and p does not divide m, then G has a subgroup of order p^α (Proof will be done with the big Sylow theorem).

Definition 3.7. Let H and K be subgroups of a group and define

$$HK = \{hk|\ h \in H,\ k \in K\}.$$

Proposition 3.8. If H and K are subgroups of a group then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Corollary 3.9. If H and K are subgroups of G then HK is a subgroup if H normalizes K (i.e. if $H \subseteq N_G(K)$).

Isomorphism Theorems

Theorem 3.10. *(First Isomorphism Theorem)* If $\varphi : G \to H$ is a homomorphism of groups, then $\ker(\varphi) \trianglelefteq G$ and $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

Corollary 3.11. Let $\varphi : G \to H$ be a homomorphism of groups.

1. φ is injective if and only if $\ker(\varphi) = id_G$.
2. $|G : \ker(\varphi)| = |\mathrm{im}(\varphi)|$.

Theorem 3.12. *(The Second or Diamond Isomorphism Theorem)* Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.

$$\begin{tikzcd}
& G \arrow[d, dash] & \\
& AB \arrow[dl, dash] \arrow[dr, dash, "\trianglerighteq"] & \\
A \arrow[dr, dash, "\trianglerighteq"] & & B \arrow[dl, dash] \\
& A \cap B \arrow[d, dash] & \\
& \{id_G\} &
\end{tikzcd}$$

Theorem 3.13. *(The Third Isomorphism Theorem)* Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

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

Theorem 3.14. *(The Fourth Isomorphism Theorem)* Let G be a group and let N be a normal subgroup of G. The there is a bijection from the set $\mathcal{S}$ of subgroups A of G which contain N onto the set $\mathcal{T}$ of subgroups of the quotient group G/N. Specifically, there is a bijective map $\varphi : \mathcal{S} \to \mathcal{T} : A \mapsto A/N$ and we have the following:

1. $A \leq B$ if and only if $A/N \leq B/N$,
2. if $A \leq B$, then $|B : A| = |B/N : A/N|$,
3. $\langle A, B\rangle/N = \langle A/N, B/N\rangle$,

4. $(A \cap B)/N = A/N \cap B/N$, and
5. $A \trianglelefteq G$ if and only if $A/N \trianglelefteq G/N$.

===============

===============

Theorem 3.15. *(Feit-Thompson)* If G is a simple group of odd order, then $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.

Definition 3.16. A group G is ***solvable*** if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, n-1$.

Theorem 3.17. The finite group G is solvable if and only if for every divisor n of $|G|$ such that $\gcd\left(n, \frac{|G|}{n}\right) = 1$, G has a subgroup of order n.

Definition 3.18. The *alternating group of degree n*, denoted by A_n, is the kernel of the sign homomorphism acting on S_n.

Proposition 3.19. The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

4. Group Actions

Definition 4.1. Let G be a group acting on a nonempty set A. For each $g \in G$ the map

$$\sigma_g : A \to A : a \mapsto g \cdot a$$

is a permutation of A. The homomorphism associated to an action of G on A

$$\varphi : G \to S_A : \varphi(g) \mapsto \sigma_g$$

is called the *permutation representation* associated to the given action.

Definition 4.2. Let G be a group acting on a set A

1. The ***kernel*** of the action is the set of elements of G that act trivially on every element of A: $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.
2. Fro each $a \in A$ the ***stabilizer*** of a in G is the set of elements of G that fix the element a: $\{g \in G \mid g \cdot a = a\}$ and is denoted by G_a.
3. An action is ***faithful*** if its kernel is the identity.

Corollary 4.3. Let G be a group acting on a set A. Two elements of G induce the same permutation on A if and only if they are in the same coset.

Proposition 4.4. Let G be a group acting on the nonempty set A. The relation on A defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.

Definition 4.5. Let G be a group acting on the nonempty set A.

1. The equivalence class $\{g \cdot a \mid g \in G\}$ is called the ***orbit*** of G containing a.

2. The action of G on A is called ***transitive*** if there is only one orbit, i.e., given any two elements $a, b \in A$ there is some $g \in G$ such that $a = g \cdot b$.

Theorem 4.6. Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

1. G acts transitively on A
2. the stabilizer in G of the point $1H \in A$ is the subgroup H
3. the kernel of the action (i.e., the kernel of π_H) is $\cap_{x\in G}\, xHx^{-1}$, and $\ker(\pi_H)$ is the largest normal subgroup of G contained in H.

Corollary 4.7. *(Cayley's Theorem)* Every group is isomorphic to a subgroup of some symmetric group. If G is of order n, then G is isomorphic to a subgroup of S_n.

Corollary 4.8. Let G be a simple, non-abelian group and let $H \leq G$. Then G is isomorphic to a subgroup of the symmetric group on G/H, $Sym(G/H)$.

Proof. Let G be a simple, non-abelian group and let $H \leq G$. Suppose that G acts on the coset space G/H by left multiplication. Obviously, this action is transitive, so we have that there is a homomorphism

$$\varphi : G \to Sym(G/H) : g \mapsto \sigma_g$$

where

$$\sigma_g : G/H \to G/H : xH \mapsto (g \cdot x)H.$$

Now, H is a proper subgroup, so $|G/H| > 1$, and since G acts transitively, we have that φ is nontrivial. This gives us that $\ker(\varphi) \neq G$, and since G is simple we get that φ is injective. ♣

Corollary 4.9. If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal. (Note: this is used mostly with subgroups of index 2)

Definition 4.10. Two elements a and b of G are said to be ***conjugate*** in G if there is some $g \in G$ such that $b = gag^{-1}$. The orbits of G acting on itself by conjugation are called *conjugacy classes* of G.

Definition 4.11. Two subsets S and T of G are said to be ***conjugate in G*** if there is some $g \in G$ such that $T = gSg^{-1}$.

Proposition 4.12. The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.

Theorem 4.13. *(The Class Equation)* Let G be a finite group and let $g_1, g_2, \dots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Theorem 4.14. *(Orbit Stabilizer Theorem)* Let G be a group acting on a set A and consider some $a \in A$. Then

$$|Orb(a)| = |G : Stab(a)|.$$

Theorem 4.15. Every normal subgroup is the union of conjugacy classes.

Definition 4.16. Let G be a group. An isomorphism from G onto itself is called an ***automorphism***. The set of all automorphisms of G is denoted by $\text{Aut}(G)$.

Proposition 4.17. Let H be a normal subgroup of G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$h \mapsto ghg^{-1} \qquad \text{for each } h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\text{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Corollary 4.18. If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

Corollary 4.19. For any subgroup H of a group G the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.

Definition 4.20. Let G be a group and let $g \in G$. Conjugation by g is called an ***inner automorphism*** of G and the subgroup of $\text{Aut}(G)$ consisting of all inner automorphisms is denoted by $\text{Inn}(G)$.

Note: For any group G we have that

$$\text{Inn}(G) \cong G/Z(G).$$

This is really useful when proving that $\text{Aut}(G)$ is nontrivial.

Definition 4.21. A subgroup H of a group G is called ***characteristic*** in G, denoted H char G, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in Aut(G)$.

Proposition 4.22. *(Properties of Characteristic Subgroups)*

1. characteristic subgroups are normal
2. if H is the unique subgroup of G of a given order, then H is characteristic in G, and
3. if K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$.

Proposition 4.23. The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, and abelian group of order $\varphi(n)$ (where φ is Euler's function).

===============

Sylow Theorems

===============

Definition 4.24. Let G be a group and let p be a prime.

1. A group of order p^α for some $\alpha \geq 0$ is called a ***p-group***. Subgroups of G which are p-groups are called ***p-subgroups***.
2. If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a ***Sylow p-subgroup*** of G.
3. The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$.

Theorem 4.25. *(Sylow's Theorem)* Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.

1. Sylow p-subgroups of G exist.

2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.

3. The number of Sylow p-subgroups in G is of the form $1 + kp$, i.e.,

$$n_p \equiv 1 \mod p.$$

   Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Lemma 4.26. Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Theorem 4.27. A nontrivial p-group has a nontrivial center.

Proof. Let G be a nontrivial p-group, and P the set of order-p elements of G. We have seen that P is nonempty, and indeed that $|P|$ is congruent to $-1 \mod p$. Now consider the action of G on P by conjugation. The stabilizer under this action of any x in P is the centralizer $C(x)$ of x, which is the subgroup of G consisting of all elements that commute with x. The orbit of x then has size $[G : C(x)]$. But G is a p-group, so $[G : C(x)]$ is a power of p. Hence $[G : C(x)]$ is either 1 or a multiple of p. Since $|P|$ is not a multiple of p, it follows that at least one of the orbits is a singleton. Then $C(x) = G$, which is to say that x commutes with every element of G. We have thus found a nontrivial element x of the center of G. ♣

Corollary 4.28. Let P be a Sylow p-subgroup of G. Then the following are equivalent:

1. P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$
2. P normal in G
3. P is characteristic in G
4. All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-subgroup.

5. Direct and Semidirect Products and Abelian Groups

Proposition 5.1. Let $G_1, G_2, \ldots, G_n$ be groups and let $G = G_1 \times G_2 \times \cdots \times G_n$ be their direct product.

1. For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i:

$$G_i \cong \{(1, 1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\}.$$

   If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. for each fixed i define $\pi_i : G \to G_i$ by

$$\pi_i((g_1, g_2, \ldots, g_n)) = g_i.$$

   Then π_i is a surjective homomorphism with

$$\begin{aligned} \ker(\pi_i) &= \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, 1) \mid g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n. \end{aligned}$$

3. Under the identifications in part (1), if $x \in G_i$ and $y \in G_j$ then $xy = yx$.

Definition 5.2.

1. A group G is *finitely generated* if there is a finite subset A of G such that $G = \langle A \rangle$.

2. For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the *free abelian group of rank r*.

Theorem 5.3. *(Fundamental Theorem of Finitely Generated Abelian Groups)* Let G be a finitely generated abelian group. Then

1. $$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$$
   for some integers $r, n_1, n_2, \ldots, n_s$ satisfying the following conditions:
   (a) $r \geq 0$ and $n_j \geq 2$ for all j, and
   (b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.
2. the expression in (1) is unique.

Definition 5.4. The integer r in the previous theorem is called the *free rank* or *Betti number* of G and the integers $n_1, n_2, \ldots, n_s$ are called the *invariant factors* of G. The description

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$$

is called the *invariant factor decomposition* of G.

Corollary 5.5. If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is the cyclic group of order n, $\mathbb{Z}/n\mathbb{Z} = Z_n$.

Theorem 5.6. Let G be an abelian group of order $n > 1$ and let the unique factorization of n distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

1. $G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$
2. for each $A \in \{A_1, A_2, \ldots, A_k\}$ with $|A| = p^\alpha$,
   $$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$$
   with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$
3. the decomposition in (1) and (2) is unique.

Definition 5.7. The integers p^{β_j} described in the preceding theorem are called the *elementary divisors* of G. The description of G given in the first two parts of the previous theorem is called the *elementary divisor decomposition* of G.

Proposition 5.8. Let $m, n \in \mathbb{Z}^+$

1. $Z_m \times Z_n \cong Z_{mn}$ if and only if $\gcd(m, n) = 1$.
2. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$

Definition 5.9. Let G be a group, let $x, y \in G$ and let A, B be nonempty subsets of G.

1. Define $[x, y] = x^{-1}y^{-1}xy$, called the *commutator* of x and y.
2. Define $[A, B] = \langle [a, b] \mid a \in A,\ b \in B \rangle$, the group generated by commutator of elements from A and B.
3. Define $G' = \langle [x, y] \mid x, y \in G \rangle$, the subgroup of G generated by the commutators of elements from G, called the *commutator subgroup* of G.

Proposition 5.10. Let G be a group, let $x, y \in G$ and let $H \leq G$. Then

1. $xy = xy[x, y]$.
2. $H \trianglelefteq G$ if and only if $[H, G] \leq H$.
3. $\sigma([x, y]) = [\sigma(x), \sigma(y)]$ for any $\sigma \in \mathrm{Aut}(G)$, G' char G, and G/G' is abelian.
4. G/G' is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$ and $H \trianglelefteq G$, then G/H is abelian.
5. If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G' i.e. $G' \leq \ker(\varphi)$ and the following diagram commutes

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\varphi"'] & G/H \arrow[d] \\ & A \end{tikzcd}$$

Proposition 5.11. Let H and K be subgroup of the group G. The number of distinct ways of writing each element of the set HK in the form hk, for some $h \in H$ and $k \in K$ is $|H \cap K|$. In particular, if $H \cap K = 1$, the each element of HK can be written uniquely as a product hk, for some $h \in H$ and $k \in K$.

Theorem 5.12. *(Product Recognition)* Suppose G is a group with subgroups H and K such that

1. H and K are normal in G, and
2. $H \cap K = 1$.

Then $HK \cong H \times K$.

Definition 5.13. If G is a group and H and K are normal subgroups of G with $H \cap K = 1$ then we call HK the *internal direct product* of H and K. We shall call $H \times K$ the *external direct product* of H and K (Note: This difference purely determines the notation of the elements of the group as these two are isomorphic by the recognition theorem).

Theorem 5.14. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. Let $\cdot$ denote the (left) action of K on H determined by φ. Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1 k_2).$$

1. This multiplication makes G into a group of order $|H||K|$.
2. The sets $\{(h, 1) \mid h \in H\}$ and $\{(1, k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1)$ for $h \in H$ and $k \mapsto (1, k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively:
$$H \cong \{(h, 1) \mid h \in H\} \quad \text{and} \quad K \cong \{(1, k) \mid k \in K\}.$$
3. $\widehat{H} = \{(h, 1) \mid h \in H\} \trianglelefteq G$
4. $\widehat{H} \cap \widehat{K} = 1$
5. for all $h \in \widehat{H}$ and $k \in \widehat{K}$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Definition 5.15. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. The group described in Theorem 5.14 is called the *semidirect product* of H and K with respect to φ and will be denoted $H \rtimes_\varphi K$ (or simply $H \rtimes K$).

Proposition 5.16. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:

1. the identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism
2. φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$
3. $K \trianglelefteq H \rtimes K$.

Theorem 5.17. Suppose G is a group with subgroups H and K such that

1. H and K are normal in G, and
2. $H \cap K = 1$.

Let $\varphi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \times K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K.

Definition 5.18. Let H be a subgroup of G. A subgroup K is called a ***compliment*** for H in G if $G = HK$ and $H \cap K = 1$.

6. Futher Topics in Group Theory

Definition 6.1. A ***maximal subgroup*** of a group G is a proper subgroup M of G such that there are no subgroups H of G such that $M < H < G$.

Theorem 6.2. Let p be a prime and let P be a group of order p^a, $a \geq 1$. Then

1. The center of P is nontrivial.
2. If H is a nontrivial normal subgroup of P then H intersects the center non-trivially. In particular, every subgroup of order p is contained in the center.
3. If H is a normal subgroup of P then H contains a subgroup of order p^b that is normal in P for each divisor p^b of $|H|$. In particular, P has a normal subgroup of order p^b for every $b \in \{1, 2, \dots, a\}$.
4. Let $H < P$ then $H < N_P(H)$.
5. Every maximal subgroup of P is of index p and is normal in P.

Definition 6.3.

1. For any (finite or infinite) group G define the following subgroups inductively

$$Z_0(G) = 1, \qquad Z_1(G) = Z(G)$$

and $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

(i.e. $Z_{i+1}(G)$ is the complete preimage in G of the center of $G/Z_i(G)$ under the natural projection). The chain of subgroups

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

is called the ***upper central series of*** G.

2. A group G is called ***nilpotent*** if $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest such c is called the *nilpotence class of* G.

Proposition 6.4. Let p be a prime and let P be a group of order p^a. Then P is nilpotent of nilpotence class at most $a - 1$ for $a \geq 2$.

Proof. For each $i \geq 0$, $P/Z_i(P)$ is a p-group, so if

$$|P/Z_i(P)| > 1 \text{ then } Z(P/Z_i(P) \neq 1$$

by Theorem 6.1 (1). Thus if $Z_i(P) \neq P$ then we have that $|Z_{i+1}(P) \geq p|Z_i(P)|$and so $|Z_{i+1}(P) \geq p^{i+1}$. In particular $|Z_a(P)| \geq p^a$, so $P = Z_a(P)$. The only way P could be of nilpotence class exactly equal to a would be if $|Z_i(P)| = p^i$ for all i. In this case, however, Z_{a-2} would have index p^2 in P, so $P/Z_{a-2}(P)$ would be abelian by Corollary 4.9. But then $P/Z_{a-1}(P)$ would equal its center and so $Z_{a-1}(P)$ would equal P $\lightning$. This proves that the class of P is $\leq a-1$. ♣

Theorem 6.5. Let G be a finite group, let $p_1, p_2, \ldots, p_s$ be the distinct primes dividing the order, and let $P_i \in Syl_{p_i}(G)$, $1 \leq i \leq s$. Then the following are equivalent:

1. G is nilpotent
2. if $H < G$ then $H < N_G(H)$
3. $P_i \trianglelefteq G$ for $1 \leq i \leq s$, i.e., every Sylow subgroup is normal in G
4. $G \cong P_1 \times P_2 \times \cdots \times P_s$.

Corollary 6.6. A finite abelian group is the direct product of its Sylow subgroups (all abelian groups are nilpotent of rank 1).

Proposition 6.7. If G is a finite group such that for all positive integers n dividing its order, G contains at most n elements x satisfying $x^n = 1$, then G is cyclic.

Proposition 6.8. *(Frattini's Argument)* Let G be a group, let H be a normal subgroup of G, and let $P \in Syl_p(H)$. Then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$.

Proposition 6.9. A finite group is nilpotent if and only if every maximal subgroup is normal.

Definition 6.10. For any (finite or infinite) group G define the following subgroups inductively:

$$G^0 = G, \qquad G^1 = [G, G], \quad \text{and} \quad G^{i+1} = [G, G^i].$$

The chain of groups

$$G^0 \geq G^1 \geq G^2 \geq \cdots$$

is called the ***lower central series of*** G.

Theorem 6.11. A group G is nilpotent if and only if $G^n = 1$ for some $n \geq 0$. More precisely, G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G is nilpotent of class c then

$$G^{c-1} \leq Z_i(G) \quad \text{for all } i \in \{0, 1, \ldots, c\}.$$

Definition 6.12. For any group G define the following sequence of subgroups inductively:

$$G^{(0)} = G, \qquad G^{(1)} = [G, G], \quad \text{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \text{for all } i \geq 1.$$

This series of subgroups is called the *derived* or *commutator* series of G.

Theorem 6.13. A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

Proof. Assume that G is solvable and so possesses a series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$$

such that each factor H_{i+1}, H_i is abelian. We prove by induction that $G^{(i)} \leq H_{s-i}$. This is true for $i = 0$, so assume that $G^{(i)} \leq H_{s-i}$. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [H_{s-i}, H_{s-i}].$$

Since G is solvable, we know that H_{s-i}/H_{s-i-1} is abelian. Moreover, $[H_{s-i}, H_{s-i}]$ is the commutator subgroup of H_{s-1}, so $H_{s-i}/[H_{s-i}, H_{s-i}]$ is the largest abelian quotient of H_{s-i} which gives us that $[H_{s-i}, H_{s-i}] \leq H_{s-i-1}$. Thus $G^{(i+1)}[H_{s-i}, H_{s-i}] \leq H_{s-i-1}$. Since $H_0 = 1$, we have that $G^{(s)} = 1$.

Conversely, if $G^{(n)} = 1$ for some $n \geq 0$ then if we take $H_i = G^{(n-i)}$ we have H_i is the largest abelian quotient of H_{i+1}. Thus the commutator series satisfies the condition for solvability. ♣

Proposition 6.14. Let G and K be groups, let H be a subgroup of G, and let $\varphi : G \to K$ be a surjective homomorphism.

1. $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. In particular, if G is solvable, then so is H.
2. $\varphi(G^{(i)}) = K^{(i)}$. In particular, homomorphic images and quotient groups of solvable groups are solvable.
3. If $N \trianglelefteq G$ and both N and G/N are solvable then so is G.

Theorem 6.15. Let G be a finite group.

1. (Burnside) If $|G| = p^a q^b$ for some primes p and q, then G is solvable.
2. (Phillip Hall) If for every prime p dividing $|G|$ we factor the order of G as $|G| = p^a m$ where $\gcd(p, m) = 1$, and G has a subgroup of order m, then G is solvable.
3. (Feit-Thompson) If $|G|$is odd then G is solvable.
4. (Thompson) If for every pair of elements $x, y \in G$, $\langle x, y\rangle$ is a solvable group, then G is solvable.

- Free Groups -

The basic idea behind a free group $F(S)$ generated by a set S is that there are no relations satisfied by any of the elements of S (in this sense S can be considered "free" of relations). Now, if we let S be an arbitrary set then a ***word*** in S is a finite sequence of elements of S. We can then define $F(S)$ to simply be the set of all words in S. We shall use this idea to carry out a formal construction of $F(S)$ for an arbitrary S below.

One of the important properties that reflects the fact that there are no relations that must be satisfied by members of S is that any *map* from the set S to a group G can be ***uniquely extended*** to a homomorphism from the group $F(S)$ to G. This is called the ***universal property*** of the free group and is what characterizes the group $F(S)$.

$$\begin{tikzcd} S \arrow[r, "inclusion"] \arrow[dr, "\varphi"'] & F(S) \arrow[d, "\Phi"] \\ & G \end{tikzcd}$$

Now, the difficulty in the construction of $F(S)$ is the proof that the word concatenation operation is both well defined and associative. If we say that S is given as a set of literals, then we can define a set S^{-1} such that there is a bijection from the set S to the set S^{-1} as given by sending $s \in S$ to its corresponding $s^{-1} \in S^{-1}$. If we then take some singleton set that is not contained in either S or S^{-1} and call it $\{1\}$. If we then join these sets we can take any $x \in S \cup S^{-1} \cup \{1\}$ and declare that $x^1 = x$. This allows us to think of words of S as finite products of members of S and their inverses. A word $s = (s_1, s_2, s_3, \ldots)$ is then said to be *reduced* if

1. $s_{i+1} \neq s_i^{-1}$ for all i with $s_i \neq 1$
2. if $s_k = 1$ for some k, then $s_i = 1$ for all $i \geq k$

The reduced word $(1, 1, 1, \ldots)$ is called the *empty word* and is denoted by 1. If we let $F(S)$ be the set of reduced words on S then we can embed S into $F(S)$ by

$$s \mapsto (s, 1, 1, 1, \ldots).$$

Under this set injection we identify S with its image and henceforth consider S as a subset of $F(S)$. We can then introduce a binary operation on the set $F(S)$ to the tune of word concatenation followed by reduction (this is pretty self-explanatory), and with the introduction of this operation we get our first theorem of this section.

Theorem 6.16. $F(S)$ is a group under the binary operation given above.

Theorem 6.17. Let G be a group, S a set and $\varphi : S \to G$ a set map. Then there is a unique group homomorphism $\Phi : F(S) \to G$ such that the following diagram commutes:

$$\begin{tikzcd} S \arrow[r, "inclusion"] \arrow[dr, "\varphi"'] & F(S) \arrow[d, "\Phi"] \\ & G \end{tikzcd}$$

Proof. If such a map were to exist, then Φ must satisfy $\Phi(s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n}) = \varphi(s_1)^{\varepsilon_1} \varphi(s_2)^{\varepsilon_2} \cdots \varphi(s_n)^{\varepsilon_n}$ if it is so be a homomorphism (which gives us uniqueness), and the fact that this actually is a homomorphism follows almost directly. ♣

Definition 6.18. The group $F(S)$ is called the *free group* on the set S. A group F is a *free group* if there is some set S such that $F = F(S)$ – in this case we call S the set of *free generators* of F. The cardinality of S is called the *rank* of the free group.

Definition 6.19. Let S be a subset of a group G such that $G = \langle S \rangle$.

1. A ***presentation*** for G is a pair (S, R), where R is a set of words in $F(S)$ such that the normal closure of $\langle R\rangle$ in $F(S)$ (the smallest normal subgroup containing $\langle R\rangle$) equals the kernel of the homomorphism $\pi : F(S) \to G$ (where π extends the identity map from S to S). The elements of S are called *generators* and those of R are called *relations* of G.

2. We say G is *finitely generated* if there is a presentation (S, R) such that S is a finites set and we say G is *finitely presented* if there is a presentation (S, R) with both S and R finite sets.

7. Introduction to Rings

Definition 7.1.

1. a ring R is a set together with two binary operations $+$ and $\times$ satisfying the following axioms
   (a) $(R, +)$ is an abelian group
   (b) $\times$ is associative
   (c) the distributive laws hold in R
2. The ring R is commutative if $\times$ is commutative
3. The ring R is said to have identity if there is an element $1 \in R$.

Definition 7.2. A ring with identity R is said to be a *division ring* if very nonzero element has a multiplicative inverse. A commutative division ring is called a *field*.

Definition 7.3.

1. A nonzero element a of R is called a *zero divisor* if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.
2. Assume that R has identity $1 \neq 0$. An element u of R is called a ***unit*** in R if there is some v in R such that $uv = vu = 1$. The set of units is denoted $R^{\times}$.

Definition 7.4. A commutative ring with identity is called an ***integral domain*** if it has no zero divisors.

Proposition 7.5. Assume that a, b, and c are elements of any ring with a not a zero divisor. If $ab = ac$ then either $a = 0$ or $b = c$.

Corollary 7.6. Any finite integral domain is a field.

Definition 7.7. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

Proposition 7.8. Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then

1. $deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$,
2. the units of $R[x]$ are just the units of R,
3. $R[x]$ is an integral domain.

Definition 7.9. Let R and S be rings.

1. A *ring homomorphism* is a map $\varphi : R \to S$ satisfying
   (a) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$, and
   (b) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$
2. The *kernel* of the ring homomorphism φ is the set of elements that map to 0_S.
3. A bijective ring homomorphism is called an isomorphism.

Proposition 7.10. Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

1. The image of φ is a subring of S.
2. The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker(\varphi)$ then $r\alpha$ and αr are in $\ker(\varphi)$ for every $r \in R$.

Definition 7.11. Let R be a ring, let I be a subset of R and let $r \in R$.

1. $rI = \{ra \mid a \in I\}$
2. A subset I of R is a ***left ideal*** of R if
   (a) I is a subring of R, and
   (b) I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$ for all $r \in R$.

   There is a similar definition for a right ideal.
3. A subset I that is both a left ideal and a right ideal is called an ideal of R.

Proposition 7.12. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r + I) + (s + I) = (r + s) + I \qquad \text{and} \qquad (r + I) \times (s + I) = (rs) + I$$

for all $r, s \in R$. Conversely if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition 7.13. When I is an ideal of R the ring R/I with the operations in the previous proposition is called the ***quotient ring*** of R by I.

Theorem 7.14.

1. *(The First Isomorphism Theorem for Ring)* If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S, and $R/\ker(\varphi)$ is isomorphic as a ring to $\varphi(R)$.
2. If I is any ideal of R, then the map

$$R \to R/I \qquad \text{defined by} \qquad r \mapsto r + I$$

   is a surjective homomorphism with kernel I. Thus every ideal is the kernel of a ring homomorphism and vice versa.

Theorem 7.15.

1. *(The Second Isomorphism Theorem for Rings)* Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A,\ b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A, and $(A + B)/B \cong A/(A \cap B)$.
2. *(The Third Isomorphism Theorem for Rings)* Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
3. *(The Fourth or Lattice Isomorphism Theorem for Rings)* Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I Furthermore, A is an ideal of R if and only if A/I is an ideal of R/I.

Definition 7.16. Let R be a ring. Then the ***characteristic*** of the ring R is the smallest number n such that $n1 = 1 + 1 + 1 + \cdots + 1 = 0$. If this never happens, then the characteristic of R is said to be 0.

Proposition 7.17. Let R be an integral domain. Then $char(R)$ is either prime or 0.

Definition 7.18. Let A be any subset of the ring R.

1. Let (A) denote the smallest ideal of R containing A, called ***the ideal generated by*** A.
2. Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$.
3. An ideal generated by a single element is called a ***principal ideal***.
4. An ideal generated by a finite set is called a ***finitely generated ideal***.

Proposition 7.19. Let I be an ideal of R.

1. $I = R$ if and only if I contains a unit.
2. Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Corollary 7.20. If R is a field then any nonzero ring homomorphism from R into another ring is an injection (the kernel of the ring homomorphism is an ideal).

Definition 7.21. An ideal M in an arbitrary ring S is called a ***maximal ideal*** if $M \neq S$ and the only ideals containing M are M and S.

Proposition 7.22. In a ring with identity every proper ideal is contained in a maximal ideal. [NB: This is important because this means ideals in a ring with identity satisfy the ascending chain condition. This becomes really important in the study of infinite rings like the power series ring $\mathbb{Z}[[x]]$.]

Proposition 7.23. Assume R is commutative. The ideal M is maximal if and only if the quotient ring R/M is a field.

Definition 7.24. Assume R is commutative. An ideal P is called a ***prime ideal*** if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

Proposition 7.25. Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Corollary 7.26. Assume R is commutative. Every maximal ideal of R is a prime ideal.

Theorem 7.27. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors, and is closed under multiplication. Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties:

1. every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R \backslash \{0\}$ then Q is a field.
2. (uniqueness of Q) The ring Q is the *"smallest"* ring containing R in which all the elements of D become units, in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Definition 7.28. Let R, D, and Q be as in the above theorem.

1. The ring Q is called the ***ring of fractions*** of D with respect to R and is denoted $D^{-1}R$.
2. If R is an integral domain and $D = R \backslash \{0\}$, Q is called the ***field of fractions*** or *quotient field* of R.

Corollary 7.29. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

Definition 7.30. The ideals A and B of the ring R are said to be ***comaximal*** if $A + B = R$.

Theorem 7.31. *(Chinese Remainder Theorem)* Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \quad \text{defined by} \quad r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $\cap A_i$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Corollary 7.32. Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$Z/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}),$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(Z/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

Corollary 7.33. Let $a, b \in \mathbb{Z}$ then

$$\mathbb{Z}/(m) \times \mathbb{Z}/(n) \cong \mathbb{Z}/(\gcd(m,n)) \times \mathbb{Z}/(\operatorname{lcm}(m,n))$$

Proof. (copied from math.stackexchange) Fix $u, v \in \mathbb{Z}$ with $un + vm = d$ (Bezout). The map

$$\mathbb{Z}_{\operatorname{lcm}(n,m)} \times \mathbb{Z}_{\gcd(n,m)} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

$$(a + \operatorname{lcm}(n,m)\mathbb{Z}, b + \gcd(n,m)\mathbb{Z}) \mapsto (ua + \tfrac{m}{d}b + m\mathbb{Z}, va - \tfrac{n}{d}b + n\mathbb{Z})$$

is well-defined(!) and clearly a group homomorphism. For the element on the left to be in the kernel, $ua + \frac{m}{d}b$ must be a multiple of m and $va - \frac{n}{d}b$ a multiple of n. But then

$$\frac{n}{d}\left(ua + \frac{m}{d}b\right) + \frac{m}{d}\left(va - \frac{n}{d}b\right) = \frac{nu + vm}{d}a = a$$

is a multiple of $\frac{nm}{d} = \operatorname{lcm}(n,m)$, i.e., we may as well assume that $a = 0$. Then $\frac{m}{d}b$ must be a multiple of m, i.e., b a multiple of d, i.e. $b \equiv 0$. We conclude that the kernel is trivial and our homomorphism injective. As both groups are finite of same order, the homomoprhism must be an isomorphism. ♣

8. Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

All rings in this section are commutative.

Definition 8.1. Any function $N : R \to \mathbb{Z}_{\geq 0}$ with $N(0) = 0$ is called a ***norm*** on the integral domain R. If $N(a) > 0$ for all $a \neq 0$ define N to be a *positive norm.*

Definition 8.2. The integral domain R is said to be a ***Euclidean Domain*** if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$ there exist elements q and r in R with

$$a = qb + r \qquad \text{with } r = 0 \text{ or } N(r) < N(b).$$

Definition 8.3. Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

1. a is said to be a ***multiple*** of b if $a = bx$ for some $x \in R$. In this case b is said to divide or be a divisor of a, written $b \mid a$.
2. A ***greatest common divisor*** of a and b is a nonzero element d such that
   (a) $d \mid a$ and $d \mid b$, and
   (b) if $d' \mid a$ and $d' \mid b$ then $d \mid d'$.

   A greatest common divisor of a and b will be denoted by $\gcd(a, b)$.

Proposition 8.4. If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.

Proposition 8.5. Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, then $d' = ud$ for some unit $u \in R$. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.

Theorem 8.6. Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then

1. d is a greatest common divisor of a and b, and
2. the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an ***R-linear combination*** of a and b, i.e., there are elements x and y in R such that

$$d = ax + by.$$

Definition 8.7. A domain R in which every ideal is principal is called a ***Principal Ideal Domain*** (PID).

Proposition 8.8. Let R be a PID and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

1. d is a greatest common divisor of a and b
2. d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R with

$$d = ax + by$$

3. d is unique up to multiplication by a unit in R.

Proposition 8.9. Every nonzero prime ideal in a PID is a maximal ideal.

Corollary 8.10. If R is any commutative ring such that the polynomial ring $R[x]$ is a PID (or Euclidean Domain), then R is necessarily a field.

Definition 8.11. Let R be an integral domain

1. Suppose $r \in R$ is nonzero and is not a unit. Then r is called ***irreducible*** if R if whenever $r = ab$ with $a, b \in R$ at least one of a or b is a unit in R.
2. The nonzero element $p \in R$ is called ***prime*** in R it the ideal (p) generated by p is a prime ideal. In other words, for any $a, b \in R$ if $p \mid ab$ then either $p \mid a$ or $p \mid b$.
3. Two elements $a, b \in R$ differing by a unit are said to be ***associate*** in R.

Proposition 8.12. In an integral domain a prime element is always irreducible.

Proposition 8.13. In a PID a nonzero element is prime if and only if it is irreducible.

Definition 8.14. A ***Unique Factorization Domain (UFD)*** is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

1. r can be written as the finite product of irreducibles p_i of R: $r = p_1 p_2 \cdots p_n$ and
2. the decomposition given in (1) is unique up to associates.

Proposition 8.15. In a UFD a nonzero element is a prime if and only if it is irreducible.

Proposition 8.16. Let a and b be two nonzero elements of the UFD R and suppose

$$a = u\, p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n} \qquad \text{and} \qquad b = v\, p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units, the primes $p_1, p_2, \ldots, p_n$ are *distinct* and the exponents e_i and f_i are ≥ 0. Then the element

$$d = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} p_3^{\min(e_3,f_3)} \cdots p_n^{\min(e_n,f_n)}$$

is a greatest common divisor of a and b.

Theorem 8.17. Every PID is a UFD. In particular, every Euclidean Domain is a UFD.

Lemma 8.18. The prime number $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1$ if and only if p is either 2 or is an odd prime congruent to $1 \mod 4$.

Proposition 8.19.

1. *(Fermat's Theorem on sums of squares)* The prime p is the sum of two integer squares, $p = a^2 + b^2$ if and only if $p = 2$ or $p \equiv 1 \mod 4$. Except for the interchanging a and b, the representation of p as the sum of two squares is unique.
2. The irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ are as follows
   (a) $1 + i$
   (b) the primes $p \in \mathbb{Z}$ with $p \equiv 3 \mod 4$
   (c) $a + bi$, $a - bi$, the distinct irreducible factors of $p = a^2 + b^2$ for the primes $p \in \mathbb{Z}$ with $p \equiv 1 \mod 4$.

9. Polynomial Rings

Proposition 9.1. Let I be an ideal of R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I. Then

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

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$

Definition 9.2. The *polynomial ring in the variables $x_1, x_2, \ldots, x_n$ with coefficients in R*, denoted $R[x_1, x_2, \ldots, x_n]$, is defined inductively by

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

Theorem 9.3. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, the there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } deg(r(x)) < deg(b(x)).$$

Proposition 9.4. *(Gauss' Lemma)* Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are some nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Corollary 9.5. Let R be a UFD, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the gcd of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Theorem 9.6. R is a UFD if and only if $R[x]$ is a UFD.

Corollary 9.7. If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

Proposition 9.8. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F.

Proposition 9.9. A polynomial of degree two or three is reducible over a field F if and only if it has a root in F.

Proposition 9.10. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$. In particular, if $p(x)$ is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

Proposition 9.11. Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$. *(Use this with $\mathbb{Z}$ AND $\mathbb{Z}/p\mathbb{Z}$ to prove irreducibility.)*

Proposition 9.12. *(Eisenstein's Criterion)* Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial in $R[x]$ where $n \geq 1$. Suppose $a_{n-1}, \ldots a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.

Proposition 9.13. The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition 9.14. Let $g(x)$ be a nonconstant monic element of $F[x]$ and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$$

be its factorization into irreducible, where the $f_i(x)$ are distinct. Then we have the following isomorphism of rings:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots F[x]/(f_k(x)^{n_k}).$$

Proposition 9.15. If the polynomial $f(x)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_k$ in F, then $f(x)$ has $(x - \alpha_1) \cdots (x - \alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable has at most n roots in F, even counted with multiplicity.

Proposition 9.16. A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, the the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Corollary 9.17. Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ in $\mathbb{Z}$, where $p_1, p_2, \ldots, p_r$ are distinct primes. We have the following isomorphism of (multiplicative) groups:

1. $(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$
2. $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$, for all $\alpha \geq 2$
3. $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$, for all odd primes p.

10. Introduction to Module Theory

Definition 10.1. Let R be a ring (not necessarily commutative nor with 1). A ***left R-module*** or a *left module over R* is a set M together with

1. a binary operation $+$ on M under which M is an abelian group, and
2. an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies
   (a) $(r+s)m = rm + sm, \quad$ for all $r, s \in R,\ m \in M$
   (b) $(rs)m = r(sm), \quad$ for all $r, s \in R,\ m \in M$, and
   (c) $r(m+n) = rm + rn, \quad$ for all $r, s \in R,\ m \in M$.

   If the ring R has 1 we impose the additional axiom:
   (d) $1m = m, \quad$ for all $m \in M$.

Definition 10.2. Let R be a ring and let M be an R-module. An ***R-submodule*** of M is a subgroup N of M which is closed under the action of ring elements.

Proposition 10.3. *(The Submodule Criterion)* Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if

1. $N \neq \varnothing$, and
2. $x + ry \in N$ for all $r \in R$ and for all $x, y \in M$.

Definition 10.4. Let R be a ring and let M and N be R-modules.

1. A map $\varphi : M \to N$ is an ***R-module homomorphism*** if it respects the R-module structures of M and N, i.e.,
   (a) $\varphi(x+y) = \varphi(x) + \varphi(y), \quad$ for all $x, y \in M$ and
   (b) $\varphi(rx) = r\varphi(x), \quad$ for all $r \in R,\ x \in M$.
2. An R-module homomorphism is an ***isomorphism*** if it is both injective and surjective. The modules M and N are said to be ***isomorphic***, denoted $M \cong N$ if there is some R-module isomorphism $\varphi : M \to N$.
3. If $\varphi : M \to N$ is an R-module homomorphism, let $\ker(\varphi) = \{m \in M \mid \varphi(m) = 0\}$ and let $\varphi(M) = \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$.
4. Let M and N be R-modules and define $\mathrm{Hom}_R(M, N)$ to be the set of R-module homomorphisms from M to N.

Proposition 10.5. Let M, N, and L be R-modules

1. A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $c, y \in M$ and $r \in R$.
2. Let $\varphi,\ \psi$ be elements of $\mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \qquad \text{for all } m \in M.$$

Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ is an abelian group. If R is a commutative ring the for $r \in R$ define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m)) \qquad \text{for all } m \in M.$$

Then $r\varphi \in \mathrm{Hom}_R(M.N)$ and with this action of the commutative ring R the abelian group $\mathrm{Hom}_R(M, N)$ is an R-module.

3. If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(L, N)$.
4. With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is an R-algebra.

Definition 10.6. The ring $\mathrm{Hom}_R(M, M)$ is called the ***endomorphism ring of*** M and will often be denoted by $\mathrm{End}_R(M)$. Elements of $\mathrm{End}(M)$ are called ***endomorphisms***.

Proposition 10.7. Let R be a ring, let M be an R-module, and let N be a submodule of M. The quotient group M/N can be made into an R-module by defining an action of elements of R by

$$r(x + N) = (rx) + N), \qquad \text{for all } r \in R,\ x + N \in M/N.$$

The natural projection map $\pi : M \to M/N$ is an R-module homomorphism with kernel N.

Definition 10.8. Let A, B be submodules of the R-module M. The *sum* of A and B is the set

$$A + B = \{a + b \mid a \in A,\ b \in B\}.$$

Definition 10.9. Let M be an R-module and let $N_1, \ldots, N_n$ be submodules of M.

1. The ***sum*** of $N_1, \ldots, N_n$ is the set of all finite sums of elements form the sets N_i : $\{a_1 + \cdots + a_n \mid a_i \in N_i\}$. Denote this sum by $N_1 + \cdots + N_n$.
2. For any subset A of M let

   $$RA = \{r_1a_1 + \cdots + r_ma_m \mid a_i \in A,\ r_i \in R,\ m \in \mathbb{Z}^+\}.$$

   If A is finite we may write $Ra_1 + Ra_2 + \cdots + Ra_m$. Call RA th ***submodule of*** M ***generated by*** A. If N is a submodule of M and $N = RA$ for some subset A of M, we call A a set of generators or a generating set for N,. and we say that N is generated by A.
3. A submodule N of M is ***finitely generated*** if there is some finites subset A of M such that $N = RA$.
4. A submodule N of M is ***cyclic*** if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element.

Proposition 10.10. Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then the following are equivalent

1. The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by

   $$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$$

   is an isomorphism (of R-modules)
2. $N_j \cap N_1 + \cdots N_{j-1} + N_{j+1} + \cdots + N_k = 0$ for all $j \in \{1, 2, \ldots, k\}$.
3. Every $x \in N_1 + \cdots + N_k$ can be written *uniquely* in the form $a_1 + a_2 + \cdots + a_k$ for $a_i \in N_i$.

Definition 10.11. If an R-module $M = N_1 + N_2 + \cdots + N_k$ is the sum of submodules $N_1, N_2, \ldots, N_k$ of M satisfying the equivalent conditions in the above proposition, then M is said to be the ***(internal) direct sum*** of $N_1, N_2, \ldots, N_k$ written

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

Definition 10.12. And R-module F is said to be ***free*** on the subset A of F if for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, for some $n \in \mathbb{Z}^+$. In this situation we say A is a ***basis*** or ***set of free generators*** for F. If R is a commutative ring the cardinality of A is called the ***rank*** of F.

Theorem 10.13. For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following ***universal property***: if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$, for all $a \in A$, that is, the following diagram commutes.

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

Corollary 10.14.

1. If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.
2. If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does in the previous theorem.

11. Vector Spaces

Definition 11.1. If F is an field and V is an F-module, then V is called a *vector space over* F.

Definition 11.2.

1. A subset S of V is called a set of ***linearly independent*** vectors if an equation $\alpha_1v_1 + \cdots + \alpha_nv_n = 0$ with $\alpha_1, \ldots \alpha_n \in F$ and $v_1, \ldots, v_n \in S$ implies $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. (Note: an infinite set is linearly independent if this condition holds for any finite subset.)
2. A *basis* of a vector space V is an ***ordered set*** of linearly independent vectors which span V. In particular, two bases sill be considered different even if one is simply a rearrangement of the other. This is sometimes referred to as an *ordered basis*.

Proposition 11.3. Assume that $\mathcal{A} = \{v_1, v_2, \ldots, v_n\}$ spans the vector space V but no proper subset of $\mathcal{A}$ spans V. Then $\mathcal{A}$ is a basis of V. In particular, any finitely generated vector space over F is a free F-module.

Theorem 11.4. *(A Replacement Theorem)* Assume $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ is a basis for V containing n elements and $\{b_1, b_2, \ldots, b_m\}$ is a set of linearly independent vectors in V. Then there is an ordering $a_1, a_2, \ldots, a_n$ such that for each kßn$\{1, 2, \ldots, m\}$ the set $\{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\}$ is a basis of V. In other words, the elements of $b_1, b_2, \ldots, b_m$ can be used to successively replace the elements of the basis $\mathcal{A}$, still retaining a basis. In particular $n \geq m$

Corollary 11.5.

1. Suppose V has a finite basis with n elements. Any set of linearly independent vectors has $\leq n$ elements. Any spanning set has $\geq n$ elements.
2. If V has some finite basis, then any two bases of V have the same cardinality.

Definition 11.6. If V is a finitely generated F-module the cardinality of any basis is called the *dimension* of V and is denoted $\dim_F(V)$, or just $\dim(V)$ when F is clear from the context, and V is said to be *finite dimensional over* F. If V is not finitely generated, V is said to be infinite dimensional.

Corollary 11.7. If A is a set of linearly independent vectors in the finite dimensional vector space V, then there exists a basis of V containing A

Theorem 11.8. If V is an n dimensional vector space over F, the $V \cong F^n$. In particular, any two finite dimensional vector spaces over F of the same dimension are isomorphic.

Proof. Let $v_1, v_2, \ldots, v_n$ be a basis for V. Define the map

$$\varphi : F^n \to V : (\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n.$$

The map φ is clearly F-linear, is surjective since the v_i span V, and is injective since the v_i are linearly independent, hence is an isomorphism. ♣

Theorem 11.9. Let V be a vector space over F and let W be a subspace of V. Then $V/W$is a vector space with $\dim(V) = \dim(W) + \dim(V/W)$.

Corollary 11.10. Let $\varphi : V \to U$ be a linear transformation of vector spaces over F. Then $\ker(\varphi)$ is a subspace of V, $\varphi(V)$ is a subspace of U, and $\dim(V) = \dim(\ker(\varphi)) + \dim(\varphi(V))$.

Corollary 11.11. Let $\varphi : V \to U$ be a linear transformation of vector spaces of the same finite dimension. Then the following are equivalent

1. φ is an isomorphism
2. φ is injective, i.e., $\ker(\varphi) = 0$
3. φ is surjective
4. φ sends a basis of V to a basis of W.

Definition 11.12. If $\varphi : V \to U$ is a linear transformation of vector spaces over F, $\ker(\varphi)$ is sometimes called the ***null space*** of φ. and the dimension of $\ker(\varphi)$ is called the ***nullity*** of φ. The dimension of $\varphi(V)$ is called the ***rank*** of φ. If $\ker(\varphi) = 0$, then the transformation is said to be ***nonsingular***.

Definition 11.13. The $m \times m$ matrix $A = (a_{ij})$ associated to the linear transformation φ is said to *represent* the linear transformation φ with respect to the bases $\mathcal{B}, \mathcal{E}$. Similarly, φ is the linear transformation represented by A with respect to the bases $\mathcal{B}, \mathcal{E}$.

Theorem 11.14. Let B be a vector space over F of dimension n and let W be a vector space over F of dimension m, with bases $\mathcal{B}, \mathcal{E}$ respectively. Then the map $\mathrm{Hom}_F(V, W) \to M_{m\times n}(F)$ from the space of linear transformations from v to W to the space of $m \times n$ matrices with coefficients in F defined by $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is a vector space isomorphism. In particular, there is a bijective correspondence between linear transformations and their associated matrices with respect to a fixed choice of bases.

Corollary 11.15. The dimension of $\mathrm{Hom}_F(V, W)$ is $(\dim(V))(\dim(W))$.

Definition 11.16. An $m \times n$ matrix A is called ***nonsingular*** if $Ax = 0$ with $x \in F^n$ implies $x = 0$.

Theorem 11.17. With notation as above $M_{\mathcal{B}}^{\mathcal{E}}(\varphi \circ \psi) = M_{\mathcal{B}}^{\mathcal{E}}(\varphi) M_{\mathcal{B}}^{\mathcal{E}}(\psi)$.

Corollary 11.18. Matrix multiplication is associative and distributive. An $n \times n$ matrix A is nonsingular if and only if it is invertible.

Corollary 11.19.

1. If $\mathcal{B}$ is a basis of the n-dimensional space V, the map $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ is a ring and a vector space isomorphism of $\text{Hom}_F(V,V)$ onto the space $M_n(F)$ of $n \times n$ matrices with coefficients in F.
2. $GL(V) \cong GL_n(F)$ where $\dim(V) = n$.

Definition 11.20. If A is any $m \times n$ matrix with entries of F, the ***row rank*** of A is the maximal number of linearly independent rows of A.

Definition 11.21. Two $n \times n$ matrices A and B are said to be ***similar*** if the is an invertible $n \times n$ matrix P such that $P^{-1}AP = B$. Two linear transformations φ and ψ from a vector space V to itself are said to be *similar* if the is a nonsingular linear transformation ξ

Definition 11.22.

1. For V any vector space over F let $V^* = \text{Hom}_F(V,F)$ be the space of linear transformations from V to F, called the ***dual space*** of V. Elements of V^* are called ***linear functionals***.
2. If $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ is a basis of the finite dimensional space V, define $v_i^* \in V^*$ for each $i = 1..n$ by its action on the basis $\mathcal{B}$:
$$v_i^*(v_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \qquad 1 \leq j \leq n.$$

Proposition 11.23. With notations as above, $\{v_1^*, v_2^*, \ldots, v_n^*\}$ is a basis of V^*. In particular, if V is finite dimensional then V^* has the same dimension as V.

Proof. (Copied from D&F) Observe that since V is finite dimensional, $\dim(V^*) = \dim(\text{Hom}_F(V,F)) = \dim(V) = n$ (Corollary 11.11), so since there are n of the v_i^*'s it suffices to prove that they are linearly independent. If
$$\alpha_1 v_1^* + \alpha_2 v_2^* + \cdots + \alpha_n v^n = 0 \quad \text{in } \text{Hom}_F(V,F),$$
then applying this element to v_i and using th equation above gives us that $\alpha_i = 0$. Since i is arbitrary these elements are linearly independent. ♣

Definition 11.24. The basis $\{v_1^*, v_2^*, \ldots, v_n^*\}$ of V^* is called the ***dual basis*** to $\{v_1, v_2, \ldots, v_n\}$.

Theorem 11.25. There is a natural injective linear transformation from V to V^{**}. If V is finite dimensional then this linear transformation is an isomorphism.

Sketch of proof. Let $v \in V$ and define the evaluation map $E_v : V^* \to F : f \mapsto f(v)$. This is a linear transformation from V^* to F, and so is an element of $\text{Hom}_F(V^*, F) = V^{**}$. This defines a natural map $\varphi : V \to V^{**} : v \mapsto E_v$. This map is injective for all V and φ is an isomorphism if V is finite dimensional.

Theorem 11.26. Let V, W be finite dimensional vector spaces over F with bases $\mathcal{B}, \mathcal{E}$, respectively and let $\mathcal{B}^*, \mathcal{E}^*$ be the dual bases . Fix some $\varphi \in \text{Hom}(V,W)$. Then for each $f \in W^*$, the composite $f \circ \varphi$ is a linear transformation from V to F, that is $f \circ \varphi \in V^*$. Thus, we can define a map $\varphi^* : W^* \to V^* : f \mapsto f \circ \varphi$ (called the ***pullback*** of f) and the matrix $M_{\mathcal{E}^*}^{\mathcal{B}^*}(\varphi^*)$ is the transpose of th matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$.

Corollary 11.27. For any matrix A, the row rank of A equals the column rank of A.

Definition 11.28.

1. A map $\varphi : V_1 \times V_2 \times \cdots \times V_n \to W$ is called ***multilinear*** if for each fixed i and fixed i and fixed elements $v_j \in V_j$, $j \neq i$, the map
$$V_i \to W \qquad \text{defined by} \qquad x \mapsto \varphi(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_n)$$

is an R-module homomorphism. If $V_i = V$, $i = 1, 2, \ldots, n$, then φ is called an *n-multilinear function on V*, and if in addition $W = R$, φ is called an *n-multilinear form on V*.

2. An n-multilinear function φ on V is called *alternating* if $\varphi(v_1, v_2, \ldots, v_n) = 0$ whenever $v_i = v_{i+1}$ for some $i \in \{1, 2, \ldots, n-1\}$. The function φ is called *symmetric* if interchanging v_i and v_j for any i and j in $(V_1, v_2, \ldots, v_n)$ does not alter the value of φ on this n-tuple.

Proposition 11.29. Let φ be an n-multilinear alternating function on V. Then

1. $\varphi(v_1, \ldots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \ldots, v_n) = -\varphi(v_1, v_2, \ldots, v_n)$ for any $i \in \{1, 2, \ldots, n-1\}$.
2. For each $\sigma \in S_n$, $\varphi(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}) = sgn(\sigma)\varphi(v_1, v_2, \ldots, v_n)$.
3. If $v_i = v_j$ for any pair of distinct $i, j \in \{1, 2, \ldots, v_n\}$ then $\varphi(v_1, v_2, \ldots, v_n) = 0$.
4. If v_i is replaced by $v_i + \alpha v_j$ in $(v_1, v_2, \ldots, v_n)$ for any $j \neq i$ and any $\alpha \in R$, the value ofφ on this n-tuple is not changed.

Proposition 11.30. Assume φ is an n-multilinear alternating function on V and that for some $v_1, v_2, \ldots, v_n$ and $w_1, w_2, \ldots, w_n \in V$ and some $\alpha_{ij} \in R$ we have

$$\begin{aligned} w_1 &= \alpha_{11}v_1 + \alpha_{21}v_2 + \cdots + \alpha_{n1}v_n \\ w_2 &= \alpha_{12}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{n2}v_n \\ &\vdots \\ w_n &= \alpha_{1n}v_1 + \alpha_{2n}v_2 + \cdots + \alpha_{nn}v_n. \end{aligned}$$

Then

$$\varphi(w_1, w_2, \ldots, w_n) = \sum_{\sigma \in S_n} sgn(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\cdots\alpha_{\sigma(n)n}\varphi(v_1, v_2, \ldots, v_n).$$

Definition 11.31. An $n \times n$ ***determinant function*** on R is any function

$$\det : M_{n\times n}(R) \to R$$

that satisfies the following two axioms:

1. det is an n-multilinear alternating form on $R^n(= V)$, where the n-tuples are the n columns of the matrices in $M_{n\times n}(R)$.
2. $\det(I) = 1$.

Theorem 11.32. There is a unique $n \times n$ determinant function on R and it can be computed for any $n \times n$ matrix (α_{ij}) by the formula:

$$det(\alpha_{ij}) = \sum_{\sigma \in S_n} sgn(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\cdots\alpha_{\sigma(n)n}$$

Corollary 11.33. The determinant is an n-multilinear function of the rows of $M_{n\times n}(R)$ and for any $n \times n$ matrix A, $\det(A) = \det(A^t)$.

Theorem 11.34. *(Cramer's Rule)* If $A_)1, A_23, \ldots, A_n$ are the columns of an $n \times n$ matrix A and $B = \beta_1 A_1 + \beta_2 A_2 + \cdots + \beta_n A_n$, for some $\beta_1, \ldots, \beta_n \in R$, then

$$\beta_i \det(A) = \det(A_1, \ldots, A_{i-1}, B, A_{i+1}, \ldots, A_n).$$

Corollary 11.35. If R is an integral domain, then $\det(R) = 0$ for $A \in M_n(R)$ if and only if the columns of A are R-linearly dependent as elements of the free R-module of rank n. Also $\det(A) = 0$ if and only if the rows of A are R-linearly dependent.

Theorem 11.36. For matrices $A, B \in M_{n\times n}(R)$, $\det(A, B) = \det(A)\det(B)$.

Definition 11.37. Let $A = (\alpha_{ij})$ be an $n \times n$ matrix. For each i, j, let A_{ij} be the $n-1 \times n-1$ matrix obtained from A by deleting its i^{th} row and j^{th} column. Then $(-1)^{i+j}\det(A_{ij})$ is called the ij ***cofactor of*** A.

Theorem 11.38. *(The Cofactor Expansion Formula along the i^{th} row)* If $A = (\alpha_{ij})$ is an $n \times n$ matrix, then for each fixed $i \in \{1, 2, \ldots n\}$ the determinant of A can be computed from the formula

$$\det(A) = (-1)^{i+1}\alpha_{i1}\det(A_{i1}) + (-1)^{i+2}\alpha_{i2}\det(A_{i2}) + \cdots + (-1)^{i+n}\alpha_{in}\det(A_{in}).$$

Theorem 11.39. *(Cofactor Formula for the Inverse of a Matrix)* Let $A = (\alpha_{ij})$ be an $n \times n$ matrix and let B be the transpose of is matrix of cofactors, i.e., $B = (\beta_{ij})$, where $\beta_{ij} = (-01)^{i+j}\det(A_{ji})$, $1 \le ii, j \le n$. Then $AB = BA = \det(A)I$. Moreover, $\det(A)$ is a unit in R if and only if A is a unit in $M_{n\times n}(R)$; in this case the matrix $\frac{1}{\det(A)}B$ is the inverse of A.

12. Modules over Principal Ideal Domains

Definition 12.1.

1. The left R module M is said to be a ***Noetherian*** R***-module*** or to satisfy the ***ascending chain condition on submodules*** if there are no infinite increasing chains of submodules (any increasing chain stabilizes).
2. The ring R is said to be *Noetherian* if it is Noetherian as a left module over itself.

Theorem 12.2. Let R be a ring and let M be a lift R-module. Then the following are equivalent:

1. M is a Noetherian R-module.
2. Every nonempty set of submodules of M contains a maximal element under inclusion.
3. Every submodule of M is finitely generated.

Corollary 12.3. If R is a PID then every nonempty set of ideal of R has a maximal element and R is a Noetherian ring.

Proposition 12.4. Let R be an integral domain and let M be a free R-module of rank $n < \infty$. Then any $n+1$ elements of M are R-linearly dependent.

Definition 12.5. For any integral domain R the ***rank*** of an R-module M is the maximum number of R-linearly independent elements of M.

Theorem 12.6. Let R be a PID, let M be a free R-module of finite rank n and let N be a submodule of M. Then

1. N is free of rank m, $M \le n$
2. there exists a basis $y_1, y_2, \ldots, y_n$ of M so that $a_1y_1, \ldots, a_my_m$ is a basis of N where $a_1, a_2, \ldots, a_m$ are nonzero elements of R with the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

Theorem 12.7. *(Fundamental Theorem, Existence: Invariant Factor Form)* Let R be a PID and let M be a finitely generated R-module.

1. Then M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and nonzero elements $a_1, a_2, \ldots, a_m$ of R which are not units in R an which satisfy the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

2. M is torsion free if and only if M is free.
3. In the decomposition in (1) the set of torsion elements,

$$\operatorname{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

(Recall: $\operatorname{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}$). In particular, M is a torsion module if and only if $r = 0$ and in this case the the annihilator of M is the ideal (a_m).

Definition 12.8. The integer r in the previous theorem is called the *free rank* or the *Betti number* of M and the elements $a_1, a_2, \ldots, a_m \in R$ are called the ***invariant factors*** of M.

Theorem 12.9. *(Fundamental Theorem, Existence: Elementary Divisor Form)* Let R be a PID and let M be a finitely generated R-module. Then M is the direct sum of a finite number of cyclic module whose annihilators are either (0) or generated by powers of the primes in R, i.e.,

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where $r \geq 0$ is an integer and $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are positive powers of (not necessarily distinct) primes in R.

Definition 12.10. Let R be a PID and let M be a finitely generated R-module as in the previous theorem. The prime powers $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are called the ***elementary divisors*** of M.

Theorem 12.11. *(The Primary Decomposition Theorem)* Let R be a PID and let M be a nonzero torsion R-module with nonzero annihilator a. Suppose the factorization of A into distinct prime powers in R is

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

and let $N_i = \{x \in M \mid p_i^{\alpha_i} x = 0\}$. $1 \leq i \leq n$. Then N_i is a submodule of M with annihilator $p_i^{\alpha_i}$ and is the submodule of M of all the elements annihilated by some power of p_i. We have

$$m \cong N_1 \oplus N_2 \oplus \oplus \cdots \oplus N_n.$$

If M is finitely generated then each N_i is the direct sum of finitely many cyclic module whose annihilators are divisors of $p_i^{\alpha_i}$.

Definition 12.12. The submodule N_i given in the previous theorem is called the *p_i-primary component* of M.

Lemma 12.13. Let R be a PID and let p be a prime in R. Let F denote the field $R/(p)$.

1. Let $M = R^r$. Then $M/pM \cong F^r$.
2. Let $M = R/(a)$ where a is a nonzero element of R. Then

$$M/pM \cong \begin{cases} F & \text{if } p \text{ divides } a \text{ in } R \\ 0 & \text{if } p \text{ does not divide } a \text{ in } R. \end{cases}$$

3. Let $M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$ where each a_i is divisible by p. Then $M/pM \cong F^k$.

Theorem 12.14. *(Fundamental Theorem, Uniqueness)* Let R be a PID.

1. Two finitely generated R-modules M_1 and M_2 are isomorphic if and only if they have the same free rank and list of invariant factors.
2. Two finitely generated R-modules M_1 and M_2 are isomorphic if and only if they have the same free rank and the same list of elementary divisors.

Corollary 12.15. Let R be a PID and let M be a finitely generated R-module.

1. The elementary divisors of M are the prime power factors of the invariant factor of M.
2. The largest invariant factor of M is the product of the larges of the distinct prime powers among the elementary divisors of M, the next largest invariant factor is the product of the largest of the distinct prime powers among the remaining elementary divisors of M, and so on.

Corollary 12.16. *(The Fundamental Theorem of Finitely Generated Abelian Groups)* See Theorem 5.3 and Theorem 5.5.

Definition 12.17.

1. An element λ of F is called an ***eigenvalue*** of a linear transformation T if there is a nonzero vector $v \in V$ such that $T(v) = \lambda v$. In this situation v is called an ***eigenvector*** of T with corresponding eigenvalue λ.
2. If A is an $n \times n$ matrix with coefficients in F, and element λ is called an *eigenvalue* of A with corresponding eigenvector v is V is a nonzero $n \times 1$ column vector such that $Av = \lambda v$.
3. If λ is an eigenvalue of the linear transformation T, the set $\{v \in V \mid T(v) = \lambda v\}$ is called the ***eigenspace*** of T corresponding to the eigenvalue λ. Similarly, if λ is an eigenvalue of the $n \times n$ matrix A, the set of $n \times 1$ matrices v with $Av = \lambda v$ is called the *eigenspace* of A corresponding to the eigenvalue λ.

Definition 12.18. The determinant of a linear transformation from V to V is the determinant of any matrix representing the linear transformation.

Proposition 12.19. The following are equivalent:

1. λ is an eigenvalue of T.
2. $\lambda I - T$ is a singular linear transformation.
3. $\det(\lambda I - T) = 0$.

Definition 12.20. Let x be an indeterminate over F. The polynomial $\det(xI - T)$ is called the ***characteristic polynomial***of T and will be denoted $c_T(x)$. If A is an $n \times n$ matrix with coefficients in F, $\det(xI - A)$ is called the *characteristic polynomial of* A and will be denoted $c_A(x)$.

Definition 12.21. The unique monic polynomial which generates the ideal $Ann(V)$ in $F[x]$ is called the ***minimal polynomial*** of T and will be denoted $m_T(x)$. The unique monic polynomial of smallest degree which when evaluated at the matrix A is the zero matrix is called the *minimal polynomial* of A and will be denoted $m_A(x)$.

Note: Since V is finite dimensional, we know that V is a finitely generated module over F. So V is torsion over $F[x]$ and we have that

$$V \cong F[x]/(a_1(x)) \oplus F[x]/(a_2(x)) \oplus \cdots \oplus F[x]/(a_m(x))$$

where the $a_i(x)$ are subject to the divisibility relations

$$a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x).$$

These $a_i(x)$ are called the invariant factors of V.

Proposition 12.22. The minimal polynomial $m_T(x)$ is the largest invariant factor of V. All the invariant factors ov V divide $m_T(x)$.

Definition 12.23. Let $a(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$ be any monic polynomial in $F[x]$. The ***companion matrix*** of $a(x)$ is the $k \times k$ matrix with 1's down the first subdiagonal, $-b_0, -b_1, \ldots, -b_{k-1}$ down the last column and zeros elsewhere. The companion matrix of $a(x)$ will be denoted $\mathcal{C}_{a(x)}$.

$$\mathcal{C}_{a(x)} = \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -b_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -b_{k-1} \end{pmatrix}$$

Definition 12.24.

1. A matrix is said to be in ***rational canonical form*** if it is the direct sum of companion matrices for monic polynomials $a_1(x), \ldots, a_m(x)$ of degree at least one with $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$. The polynomials $a_i(x)$ are called the *invariant factors* of the matrix. Such a matrix is also said to be a ***block diagonal*** matrix with block of the companion matrices for the $a_i(x)$.

$$\begin{pmatrix} \mathcal{C}_{a_1(x)} & & & \\ & \mathcal{C}_{a_1(x)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{a_m(x)} \end{pmatrix}$$

2. A ***rational canonical form*** for a linear transformation T is a matrix representing T which is in rational canonical form.

Theorem 12.25. *(Rational Canonical Form for Linear Transformations)* Let V be a finite dimensional vector space over the field F and let T be a linear transformation of V.

1. There is a basis for V with respect to which the matrix for T is in rational canonical form.
2. The rational canonical form is unique

Theorem 12.26. Let S and T be linear transformations of V. Then the following are equivalent:

1. S and T are similar linear transformations
2. the $F[x]$-modules obtained from V via S and via T are isomorphic $F[x]$-modules
3. S and T have the same rational canonical form.

Theorem 12.27. *(Rational Canonical Form for Linear Transformations)* Let A be a $n \times n$ matrix over a filed F.

1. The matrix A is similar to a matrix in rational canonical form.
2. The rational canonical form of A is unique.

Definition 12.28. The *invariant factors* of an $n \times n$ matrix over a field F are the invariant factors of its rational canonical form.

Theorem 12.29. Let A and B be $n \times n$ matrices over a field F. Then A and B are similar if and only if A and B have the same rational canonical form.

Corollary 12.30. Let A and B be two $n \times n$ matrices over a field F and suppose F is a subfield of the field K.

1. The rational canonical form of A is the same whether it is computed over K or over F. The minimal and characteristic polynomials and the invariant factors of A are the same whether A is considered as a matrix over F or as a matrix over K.
2. The matrices A and B are similar over K if and only if they are similar over F.

Lemma 12.31. Let $a(x) \in F[x]$ be any monic polynomial.

1. The characteristic polynomial of the companion matrix of $a(x)$ is $a(x)$.
2. If M is the block diagonal matrix
$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}$$
given by the direct sum of matrices $A_1, A_2, \ldots, A_k$ then the characteristic polynomial of M is the product of the characteristic polynomials of $A_1, A_2, \ldots, A_k$.

Proposition 12.32. Let A be an $n \times n$ matrix over the field F.

1. The characteristic polynomial of A is the product of all the invariant factors of A.
2. *(The Cayley-Hamilton Theorem)* The minimal polynomial of A divides the characteristic polynomial of A.
3. The characteristic polynomial of A divides some power of the minimal polynomial of A. In particular these polynomials have the same roots, not counting multiplicities.

Theorem 12.33. Let A be an $n \times n$ matrix over the field F. Using the three elementary rows and column operations, the $n \times n$ matrix $xI - A$ with entries from $F[x]$ can be put into the diagonal ***Smith Normal Form*** given by
$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a_1(x) & & & \\ & & & & a_2(x) & & \\ & & & & & \ddots & \\ & & & & & & a_m(x) \end{pmatrix}$$

Definition 12.34. The $k \times k$ matrix with λ along the main diagonal and 1 along the first superdiagonal is called the $k \times k$ *elementary Jordan matrix with eigenvalue* λ or the *Jordan block of size* k *with eigenvalue* λ.

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$

Definition 12.35.

1. A matrix is said to be in ***Jordan canonical form*** if it is a block diagonal matrix with Jordan blocks along the diagonal.
2. A ***Jordan canonical form*** for a linear transformation T is a matrix representing T which is in Jordan canonical form.

Theorem 12.36. *(Jordan Canonical Form for Linear Transformations)* Let V be a finite dimensional vector space over the field F and let T be a linear transformation of V. Assume that F contains all the eigenvalues of T.

1. There is a basis for V with respect to which the matrix for T is in Jordan canonical form.
2. The Jordan canonical for for T is unique up to a permutation of the Jordan blocks along the diagonal.

Theorem 12.37. *(Jordan Canonical Form for Matrices)* Let A be a $n \times n$ matrix over the field F and assume that F contains all the eigenvalues of A.

1. The matrix A is similar to a matrix in Jordan canonical form.
2. The Jordan canonical for for A is unique up to a permutation of the Jordan blocks along the diagonal.

Corollary 12.38.

1. If a matrix A is similar to a diagonal matrix D, then D is the Jordan canonical form of A.
2. Two diagonal matrices are similar if and only if their diagonal entries are the same up to a permutation.

Corollary 12.39. If A is an $n \times n$ matrix with entries from F and F contains all the eigenvalues of A, then A is similar to a diagonal matrix over F if and only if the minimal polynomial of A has no repeated roots.

13. Field Theory

Definition 13.1. The *characteristic* of a field F, denoted $ch(F)$, is defined to be the smallest positive integer p such that $p \cdots 1_F = 0$ if such a p is defined to be 0 otherwise.

Proposition 13.2. The characteristic of a field F, $ch(F)$ is either 0 or a prime p. If $ch(F) = p$ then for any $\alpha \in F$,

$$p \cdot \alpha = \underbrace{\alpha + \alpha + \cdots + \alpha}_{p \text{ times}} = 0.$$

Definition 13.3. The ***prime subfield*** of a field F is the subfield of F generated by the multiplicative identity 1_F of F. It is (isomorphic to) either $\mathbb{Q}$ or $\mathbb{F}_p$.

Definition 13.4. If K is a field containing the subfield F, then K is said to be an ***extension field*** of F, denoted K/F or by the digram

$$\begin{array}{c} K \\ | \\ F \end{array}$$

In particular, every field F is an extension of its prime subfield. The field F is sometimes called the ***base field*** of the extension.

Definition 13.5. The ***degree*** (or ***relative degree*** or ***index***) of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F. The extension is said to be ***finite*** if the degree of K is finite and infinite otherwise.

Proposition 13.6. Let $\varphi : F \to F'$ be a homomorphism of fields. Then φ is either identically 0 or is injective, so that the image of φ is either 0 or isomorphic to F.

Theorem 13.7. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy show that there exists an extension of F in which $p(x)$ has a root.

Theorem 13.8. Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta = x \mod (p(x)) \in K$. Then the elements

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

are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $[K : F] = n$. Hence

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

consists of all polynomials of degree $< n$ in θ.

Corollary 13.9. Let K be as in the previous theorem, and let $a(\theta), b(\theta) \in K$. be two polynomials of degree $< n$ in θ. Then addition in K is defined simply by the usual polynomial addition and multiplication in K is defined by

$$a(\theta)b(\theta) = r(\theta)$$

where $r(x)$ is the remainder obtained after dividing the polynomial $a(x)b(x)$ by $p(x)$ in $F[x]$.

Definition 13.10. Let K be an extension of the field F and let $\alpha, \beta, \ldots \in K$ be a collection of elements of K. Then the smallest subfield of K containing both F and the elements of $\alpha, \beta, \ldots$ denoted $F(\alpha, \beta, \ldots)$ is called the field ***generated by*** $\alpha, \beta, \ldots$ ***over*** F.

Definition 13.11. If the field K is generated by a single element α over F, $K = F(\alpha)$, then K is said to be a ***simple*** extension of F and the element α is called a ***primitive element*** for the extension.

Theorem 13.12. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$: $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then

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

Corollary 13.13. Suppose in the previous theorem that $p(x)$ is of degree n. Then

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots a_{n-1}\} \subseteq K.$$

Theorem 13.14. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ and let β be a root of $p'(x)$. Then there is an isomorphism

$$\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$$

$$\alpha \longmapsto \beta$$

Definition 13.15. The element $\alpha \in K$ is said to be ***algebraic*** over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F then α is said to be ***transcendental*** over F. The extension K/F is said to be *algebraic* if every element of K is algebraic over F.

Note: If K is algebraic then it is not necessarily true that K is finite. Consider the set A of all algebraic numbers over $\mathbb{Q}$. Then $\mathbb{Q}(A)$ is algebraic but is certainly not finite.

Proposition 13.16. Let α be algebraic over F. Then there is a unique, monic, irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Corollary 13.17. If L/F is an extension of fields and α is algebraic over both F and L, then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

Definition 13.18. The polynomial $m_{\alpha,F}(x)$ is called the ***minimal polynomial*** for α over F. The *degree* of $m_\alpha(x)$ is called the *degree* of α.

Proposition 13.19. Let α be algebraic over the field F and let $F(\alpha)$ be the field generated by α over F. Then

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

so that in particular

$$[F(\alpha) : F] = \deg(m_\alpha(x)) = \deg 9\alpha),$$

i.e., the degree of α over F is the degree of the extension it generates over F.

Proposition 13.20. The element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite.

Corollary 13.21. If the extension K/F is finite, then it is algebraic.

Theorem 13.22. Let $F \subseteq K \subseteq L$ be fields. Then

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

Corollary 13.23. Suppose L/F is a finite extension and let K be any subfield of L containing F, $F \subseteq K \subseteq L$. Then $[K : F]$ divides $[L : F]$.

Definition 13.24. Am extension K/F is ***finitely generated*** if there are elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ in K such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Lemma 13.25. $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Theorem 13.26. The extension K/F is finite if an only if K is generated by a finite number of algebraic elements over F. More precisely, a field generated over F by a finite number of algebraic elements of degrees $n_1, n_2, \ldots, n_k$ is algebraic of degree $\leq n_1 n_2 \cdots n_k$.

Corollary 13.27. Suppose α and β are algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β (for $\beta \neq 0$), are all algebraic.

Corollary 13.28. Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.

Theorem 13.29. If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

Definition 13.30. Let K_1 and K_2 be two subfields of a field K. Then the ***composite field*** of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2. Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.

Proposition 13.31. Let K_1 and K_2 be two finite extensions of a field F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_m$ are bases for K_1 and K_2 over F, respectively, then the elements $\alpha_i\beta_j$ for $i = 1..n$ and $j = 1..m$ span K_1K_2 over F.

By this proposition, we have the following diagram

$$\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash, "\leq m"'] \arrow[dr, dash, "\leq n"] & \\
K_1 \arrow[dr, dash, "n"'] & & K_2 \arrow[dl, dash, "m"] \\
 & F &
\end{tikzcd}$$

Corollary 13.32. Suppose that $[K_1 : F] = n,\ [K_2 : F] = m$ in the previous proposition, where m and n are relatively prime. Then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

Proposition 13.33. If the element $\alpha \in \mathbb{R}$ is obtained from a field $F \subset \mathbb{R}$ by a series of straightedge and compass constructions then $[F(\alpha) : F] = 2^k$ for some integer $k \geq 0$.

Definition 13.34. The extension field K of F is called a ***splitting field*** for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Theorem 13.35. For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting filed for $f(x)$.

Definition 13.36. If K is an algebraic extension of F which is the splitting field over F for a collection of polynomials $f(x) \in F[x]$ then K is called a ***normal extension*** of F.

Proposition 13.37. A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.

Definition 13.38. A generator of the cyclic group of all n^{th} roots of unity is called a ***primitive*** n^{th} root of unity.

Definition 13.39. The field $\mathbb{Q}(\zeta_n)$ is called the ***cyclotomic field of n^{th} roots of unity***.

Theorem 13.40. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma : E \xrightarrow{\sim} E'$, i.e., σ restricted to F is the isomorphism φ:

$$\begin{tikzcd}
\sigma : & E \arrow[r, "\sim"] \arrow[d, dash] & E' \arrow[d, dash] \\
\varphi : & F \arrow[r, "\sim"] & F'
\end{tikzcd}$$

Corollary 13.41. *(Uniqueness of Splitting Fields)* Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.

Definition 13.42. The field $\overline{F}$ is called an ***algebraic closure*** of F if $\overline{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$.

Definition 13.43. A filed K is said to be ***algebraically closed*** if every polynomial with coefficients in K has root in K.

Proposition 13.44. Let $\overline{F}$ be an algebraic closure of F. Then $\overline{F}$ is algebraically closed.

Proposition 13.45. For any filed F there exists an algebraically closed field K containing F.

Proposition 13.46. Let K be an algebraically closed field and let F be a subfield of K. Then the collection of elements $\overline{F}$ of K that are algebraic over F is an algebraic closure of F. An algebraic closure is unique up to isomorphism.

Definition 13.47. A polynomial over F is called ***separable*** if has no multiple roots. A polynomial which is not separable is called ***inseparable***.

Definition 13.48. The ***derivative*** of the polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

is defined to be the polynomial

$$D_x f(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x].$$

Proposition 13.49. A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative $\gcd(f(x), D_x f(x)) = 1$.

Corollary 13.50. Every *irreducible* polynomial over a field of characteristic 0 is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.

Proposition 13.51. Let F be a field of characteristic o. Then for any $a, b \in F$,

$$(a+b)^p = a^p + b^p, \quad \text{and} \quad (ab)^p = a^p b^p.$$

Put another way, the p^{th}-power map defined by $\varphi(a) = a^p$ is an injective field homomorphism from F to F. This map is called the ***Frobenius endomorphism*** of F.

Corollary 13.52. Suppose that $\mathbb{F}$ is a finite field of characteristic p. Then every element of $\mathbb{F}$ is a p^{th} power in $\mathbb{F}$ (notationally $\mathbb{F} = \mathbb{F}^p$).

Proposition 13.53. Every irreducible polynomial over a finite field $\mathbb{F}$ is separable. A polynomial in $\mathbb{F}[x]$ is separable if an only if it is the product of distinct irreducible polynomials in $\mathbb{F}[x]$.

Definition 13.54. A filed K of characteristic p is called ***perfect*** if every element of K is a p^{th} power in K, i.e., $K = K^p$. Any field of characteristic 0 is also called perfect.

Proposition 13.55. Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. Then there is a unique integer $k \geq 0$ ans a unique irreducible, separable polynomial $p_{sep}(x) \in F[x]$ such that

$$p(x) = p_{sep}(x^{p^k}).$$

Definition 13.56. Let $p(x)$ be an irreducible polynomial over field of characteristic p. The degree $p_{sep}(x)$ in the last proposition is called the ***inseparable degree*** of $p(x)$, denoted $deg_i(p(x))$.

Definition 13.57. The field K is said to ***separable*** over F if every element of K is the root of a separable polynomial over F. A field which is not separable is ***inseparable***.

Corollary 13.58. Every finite extension of a perfect field is separable. In particular, every finite extension of either $\mathbb{Q}$ or a finite field is separable.

Definition 13.59. Let μ_n denote that ***group of n^{th} roots of unity over*** $\mathbb{Q}$.

Definition 13.60. Define the n^{th} ***cyclotomic polynomial*** $\Phi_n(x)$ to be the polynomial whose roots are primitive n^{th} roots of unity:

$$\Phi_n(x) = \prod_{\zeta \text{ primitive } \in \ \mu_n} (x - \zeta) = \prod_{\substack{1 \leq a \leq n \\ (a,n)=1}} (x - \zeta_n^a)$$

(which is of degree $\varphi(n)$ for the Euler φ).

Lemma 13.61. The cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Theorem 13.62. The cyclotomic polynomial $\Phi_n(x)$ is an irreducible, monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Corollary 13.63. The degree over $\mathbb{Q}$ of the cyclotomic field of n^{th} roots of unity is $\varphi(n)$:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

14. Galois Theory

Definition 14.1.

1. An isomorphism σ of K with itself is called an ***automorphism*** of K. The collection of automorphisms of K is denoted $\mathrm{Aut}(K)$. If $\alpha \in K$ we shall write $\sigma\alpha$ for $\sigma(\alpha)$.
2. An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to ***fix*** an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If F is a subset of K, then an automorphism σ is said to ***fix*** F if it fixes all the elements of F.

Definition 14.2. Let K/F be an extension of fields. Let $\mathrm{Aut}(K/F)$ be the collections of automorphisms of K which fix F.

Proposition 14.3. $\mathrm{Aut}(K)$ is a group under composition and $\mathrm{Aut}(K/F)$ is a subgroup.

Proposition 14.4. Let K/F be a field extension and let $\alpha \in K$ be an algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α over F, i.e., $\mathrm{Aut}(K/F)$ permutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficients in F having α as a root also has $\sigma\alpha$ as a root.

Proposition 14.5. Let $H \leq \mathrm{Aut}(K)$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all elements of H is a subfield of K.

Definition 14.6. If H is a subgroup of the group of automorphisms of K, the subfield of K fixed by all elements of H is called the ***fixed field*** of H.

Proposition 14.7. The association of groups to fields and fields to groups defined above is inclusion reversing, namely

1. if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$, and
2. if $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2, respectively, then $F_2 \subseteq F_1$.

Proposition 14.8. Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then

$$|\mathrm{Aut}(E/F)| \leq [E : F]$$

with equality if $f(x)$ is separable over F.

Definition 14.9. Let K/F be a finite extension. Then K is said to be ***Galois*** over F and K/F is a ***Galois extension*** if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois the group of automorphisms $\mathrm{Aut}(K/F)$ is called the ***Galois group*** of K/F, denoted $\mathrm{Gal}(K/F)$.

Corollary 14.10. If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.

Definition 14.11. If $f(x)$ is a separable polynomial over F, then the ***Galois group of*** $f(x)$ ***over*** F is the Galois group of the splitting field of $f(x)$ over F.

Definition 14.12. A ***character*** χ of a group G with values in a field L is a homomorphism from G to the multiplicative group of L:

$$\chi : G \to L^{\times}$$

i.e., $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$ and $\chi(g)$ is a nonzero element of L for all $g \in G$.

Definition 14.13. The characters $\chi_1, \chi_2, \cdots, \chi_n$ of G are said to be ***linearly independent*** over L if they are linearly independent as functions on G, i.e., if there is no nontrivial relation

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$$

as a function on G (that is, $a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$ for all $g \in G$).

Theorem 14.14. *(Linear Independence of Characters)* If $\chi_1, \chi_2, \cdots, \chi_n$ are distinct characters of G with values in L then they are linearly independent over L.

Corollary 14.15. If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct embeddings (injective homomorphisms) of a field K into a field L, then they are linearly independent as functions on K. In particular distinct automorphisms of a field K are linearly independent as functions on K.

Theorem 14.16. Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgorup of the automorphisms of a field K and let F be the fixed field. Then

$$[K : F] = n = |G|.$$

Corollary 14.17. Let K/F be any finite extension. Then

$$|\mathrm{Aut}(K/F)| \le [K : F]$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. Put another way, K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof. Let F_1 be the fixed field of $\mathrm{Aut}(K/F)$. Then since every $\sigma \in \mathrm{Aut}(K/F)$ fixes F, we have that

$$F \subseteq F_1 \subseteq K.$$

By Theorem 14.9 we then get that $[K : F_1] = |\mathrm{Aut}(K/F)|$. Hence $[K : F] = |\mathrm{Aut}(K/F)|[F_1 : F]$. ♣

Corollary 14.18. Let G be a finite subgroup of automorphisms of a field K and let F be the fixed field. Then every automorphism of K fixing F is contained in G, i.e, $\mathrm{Aut}(K/F) = G$, so that K/F is Galois, with Galois group G.

Corollary 14.19. If $G_1 \ne G_2$ are distinct finite subgroups of automorphisms of a field K then their fixed fields are also distinct.

Theorem 14.20. The extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. Furthermore, if this is the case then every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K (so in particular K/F is a separable extension).

Definition 14.21. Let K/F be a Galois extension. If $\alpha \in K$ the elements $\sigma\alpha$ for σ in $\mathrm{Gal}(K/F)$ are called ***conjugates*** (or ***Galois conjugates***) of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the ***conjugate field*** of E over F.

Note. We now have 4 characterizations of Galois extensions K/F:

1. splitting fields of separable polynomials over F
2. fields where F is precisely the set of elements fixed by $\mathrm{Aut}(K/F)$
3. fields with $[K : F] = |\mathrm{Aut}(K/F)|$
4. finite, normal, separable extensions.

Theorem 14.22. ***(Fundamental Theorem of Galois Theory)*** Let K/F be a Galois extension and set $G = \mathrm{Gal}(K/F)$. Then there is a bijection

$$\left\{ \begin{array}{cc} & \mathrm{K} \\ \text{subfields E} & | \\ \text{of K} & \mathrm{E} \\ \text{containing F} & | \\ & \mathrm{F} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{cc} & 1 \\ \text{subgroups H} & | \\ \text{of G} & \mathrm{H} \\ & | \\ & \mathrm{G} \end{array} \right\}$$

given by the correspondences

$$\begin{array}{ccc} E & \longrightarrow & \left\{ \begin{array}{c} \text{the elements of G} \\ \text{fixing E} \end{array} \right\} \\ \left\{ \begin{array}{c} \text{the fixed field} \\ \text{of H} \end{array} \right\} & \longleftarrow & H \end{array}$$

which are inverse to each other. Under this correspondence,

1. (inclusion reversing) If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \le H_1$

2. $[K : E] = |H|$ and $[E : F] = |G : H|$, the index of H in G:

$$\begin{array}{ccc} K & & \\ | & \} & |H| \\ E & & \\ | & \} & |G:H| \\ F & & \end{array}$$

3. K/E is always Galois, with Galois group $\mathrm{Gal}(K/E) = H$:

$$\begin{array}{cc} K & \\ | & H \\ E & \end{array}$$

4. E is Galois over F if and only H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group
$$\mathrm{Gal}(E/F) \cong G/H.$$
More generally, even if H is not necessarily normal in G, the isomorphisms of E which fix F are in one to one correspondence with the cosets $\{\sigma H\}$ of H in G.

5. If E_1, E_2 correspond to H_1, H_2, respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2\rangle$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Hence the lattice of subfields of K containing F and the lattice of subgroups of F are "dual" (the lattice diagram for one is the lattice diagram for the other turned upside down).

Proposition 14.23. Any finite field is isomorphic to $\mathbb{F}^{p^n}$ for some prime p and some integer $n \geq 1$. The field $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of the polynomial $x^{p^n} - x$, with cyclic Galois group of order n generated by the Frobenius automorphism σ_p. The subfields of $\mathbb{F}_{p^n}$ are all Galois over $\mathbb{F} - p$ and are in one to one correspondence with the divisors d of n. They are the fields $\mathbb{F}_{p^d}$, the fixed fields of σ_p^d.

Corollary 14.24. The irreducible polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime p.

Proposition 14.25. The finite field $\mathbb{F}_{p^n}$ is a simple extension of $\mathbb{F}_p$. In particular, there exists an irreducible polynomial of degree n over $\mathbb{F}_p$ for every $n \geq 1$.

Proposition 14.26. The polynomial $x^{p^n} - x$ is precisely the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where d runs through all the divisors of n.

Proposition 14.27. Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension, with Galois group
$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$$
isomorphic to a subgroup of $\mathrm{Gal}(K/F)$. Pictorially,

$$\begin{tikzcd} & KF' \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash] & & F' \arrow[dl, dash] \\ & K \cap F' \arrow[d, dash] & \\ & F & \end{tikzcd}$$

Corollary 14.28. Suppose K/F is a Galois extension and F'/F is any finite extension. Then

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Proposition 14.29. Let K_1 and K_2 be Galois extensions of a field F. Then

1. The intersection $K_1 \cap K_2$ is Galois over F.
2. The composite K_1K_2 is Galois over F. The Galois group is isomorphic to the subgroup

$$H = \{\langle \sigma, \tau \rangle \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

of the direct product $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to the intersection $K_1 \cap K_2$ are equal.

$$\begin{tikzcd}[column sep=small]
 & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & K_1 \cap K_2 \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

Corollary 14.30. Let K_1 and K_2 be Galois extensions of a field F with $K_1 \cap K_2 = F$. Then

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Conversely, if K is Galois over F and $G = \mathrm{Gal}(K/F) = G_1 \times G_2$ is the direct product of two subgroups G_1 and G_2, then K is the composite of two Galois extensions K_1 and K_2 of F with $K_1 \cap K_2 = F$.

Corollary 14.31. Let E/F be any finite, separable extension. Then E is contained in an extension K which is Galois over F and is minimal in the sense that in a fixed algebraic closure of K any other Galois extension of F containing E contains K.

Definition 14.32. The Galois extension K of F containing E in the previous corollary is called the ***Galois closure*** of E over F.

Proposition 14.33. Let K/F be a finite extension. Then $K = F(\theta)$ if and only if there exist finitely many subfields of K containing F.

Theorem 14.34. *(The Primitive Element Theorem)* If K/F is finite and separable, then K/F is simple. In particular, any finite extension of fields of characteristic 0 is simple.

Theorem 14.35. The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity s isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism is give explicitly by the map

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \mod n &\longmapsto \sigma_a \end{aligned}$$

where σ_a is the automorphism defined by

$$\sigma_a(\zeta_n) = \zeta_n^a.$$

Corollary 14.36. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the decomposition of the positive integer n into distinct prime powers. The the cyclotomic fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$, $i = 1..k$ intersect only in the field $\mathbb{Q}$ and their composite is the cyclotomic field $\mathbb{Q}(\zeta_n)$. We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_2^{a_2}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q})$$

which under the isomorphism given in the previous theorem is the Chinese Remainder Theorem

$$(Z/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

Definition 14.37. The extension K/F is called an ***abelian*** extension if K/F is Galois and $\mathrm{Gal}(K/F)$ is an abelian group.

Corollary 14.38. Let G be any finite abelian group. Then there is a subfield K of a cyclotomic field with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

Theorem 14.39. *(Kronecker-Weber)* Let K be a finite abelian extension of $\mathbb{Q}$. Then K is contained in a cyclotomic extension of $\mathbb{Q}$.

Proposition 14.40. The regular n-gon can be constructed by straightedge and compass if and only if $n = 2^k p_1 \cdots p_r$ is the porduct of a power of 2 and distinct Fermat primes.

Note: Fermat primes are primes of the form $2^{2^n} + 1$.