Kayla Orlinsky

Algebra Exam Cheat Sheet

This color corresponds to Group and Field Theory
This color corresponds to Ring and Module Theory

Group Classification Theory

Theorem 1. *Isomorphism Theorems*

$$G/\ker(\varphi) \cong \mathfrak{Im}(\varphi) \qquad H/N \cap H \cong NH/N \qquad (G/K)/(H/K) \cong G/H$$

Theorem 2. *Sylow Theorems*

If: $|G| < \infty$

Then:

(1) Sylow p-subgroups exist for all p

(2) For fixed p, Sylow p-subgroups are conjugates

(3) The number of Sylow p-subgroups n_p satisfies the following:

- $n_p \equiv 1 \mod p$
- If $G = p^n m$ where $\gcd(p, m) = 1$, then n_p divides m
- $n_p = [G : N_G(P)]$

Theorem 3. *Recognizing Direct Products*

$G \cong H \times K$ $\iff$

-
- G has two normal subgroups H, K
- $HK = G$
- $H \cap K = \{e\}$

Theorem 4. *Recognizing Semi-Direct Products*

If:

- G has a subgroup H and a normal subgroups N
- $HN = G$
- $H \cap N = \{e\}$

Then: $G \cong N \rtimes_\varphi H$ assuming there exists a non-trivial homomorphism $\varphi : H \to \text{Aut}(N)$.

***Note that if a semi-direct product exists, then its multiplication is given by $nhn^{-1} = \varphi(h)(n)$ for $h \in H$, $n \in N$.

Theorem 5. *Isomoprhic Semi-Direct Products*

Given $N \rtimes_{\varphi_1} H$ and $N \rtimes_{\varphi_2} H$ with $\varphi_1, \varphi_2 : H \to \text{Aut}(N)$

If:

- there exists an automorphism $\sigma : H \to H$ such that $\varphi_1 \circ \sigma = \varphi_2$
- *OR* there exists an automorphism $\alpha : N \to N$ so
  $\varphi_1(h) = \alpha \circ \varphi_2(h) \circ \alpha^{-1}$ for all $h \in H$
- *OR* a there exists both σ and α so $(\varphi_1 \circ \sigma)(h) = \alpha \circ \varphi_2(h) \circ \alpha^{-1}$ for all $h \in H$

Then:

$$N \rtimes_{\varphi_1} H \cong N \rtimes_{\varphi_2} H$$

Example 1.

Determine all semi-direct products up to isomorphism of $\mathbb{Z}_{15} \rtimes \mathbb{Z}_{67}$

First, let $\mathbb{Z}_3 \cong \langle a \rangle$, $\mathbb{Z}_5 \cong \langle b \rangle$, and $\mathbb{Z}_{67} \cong \langle c \rangle$.

Then since $\text{Aut}(\mathbb{Z}_{67}) \cong \mathbb{Z}_{66}$ we have that $\varphi(b) = \text{id}$ since 5 does not divide the order of $\mathbb{Z}_{66}$ and $\varphi(a) = \alpha$ where α has order 3.

Since $\mathbb{Z}_{66}$ is abelian, there are exactly two non-trivial options for α and one will be the square of the other. Namely, if $\varphi_1(a) = \alpha$ and $\varphi_2(a) = \alpha^2$, then $\varphi_1(a^2) = \varphi_2(a)$ and since $a \mapsto a^2$ is an automorphism of $\mathbb{Z}_3$, these will generate isomorphic semi-direct products.

One can check that $\alpha^3(c) = \alpha^2(c^{29}) = \alpha(c^{37}) = c$ has order 3 and defines multiplication for G given by $bcb^{-1} = \varphi(b)(c) = c$ and $aca^{-1} = \varphi(a)(c) = c^{29}$.

Thus, $\mathbb{Z}_{15} \rtimes \mathbb{Z}_{67} \cong \langle a, b, c \,|\, a^3 = b^5 = c^{67} = 1, ab = ba, bc = cb, ac = c^{29}a \rangle$.

Theorem 6. *Classification of Finitely Generated Abelian Groups*

If: G is a finitely generated abelian group

Then:

$$G \cong \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_m} \qquad n_i | n_{i+1} \forall i.$$

***Note that it is possible to break each of the $\mathbb{Z}_{n_i}$ into its prime power divisors and reorder, however, the primes may not be distinct.
For example, $\mathbb{Z}_{12} \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3$ which is of course different from $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Definition 1. *Solvable Groups*

A group G is solvable if there exists a subnormal series

$$\{e\} \trianglelefteq G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G \qquad G_{i-1}/G_i \text{ abelain } \forall i$$

Lemma 1. *Facts about Solvable Groups*

- Subgroups and quotients of solvable groups are solvable
- If N is normal in G and solvable, and G/N is solvable, then G is solvable
- S_n is not solvable for $n \geq 5$ (S_3 and S_4 are solvable)

Lemma 2. *Useful Results that Should be Reproved*

For $|G| < \infty$

- If P is a Sylow p-subgroup of a normal subgroup $N \trianglelefteq G$ and $P \trianglelefteq N$, then P is normal in G.
- If p is the smallest prime dividing $|G|$, then any subgroup of index p is normal in G.

Lemma 3. *Crucial (and Citeable) Results*

For $|G| < \infty$

- The product of a subgroup and a normal subgroup is again a subgroup
- If $|HK| = \frac{|H||K|}{|H \cap K|} = |G|$ then $HK = G$ even if neither H nor K is normal

- From the class equation: p-groups (groups of order p^n for p prime) have non-trivial centers.
- Inductively on the previous result: p-groups are solvable
- Groups of order p^2 are abelian
- Groups of order pq where p does not divide $q-1$ are abelian
- If all of the Sylow subgroups of G are normal, then G is a direct product of its Sylow subgroups.

Lemma 4. *Facts about the Symmetric Group*

In S_n:

- Any cycle σ can be written as a product of transpositions: an even number of transpositions means σ is even, an odd number of transpositions means σ is odd
- A k-cycle is even when k is odd, and odd when k is even
- A product of two even permutations is even
- A product of two odd permutations is odd
- A product of an even permutation and an odd permutation is odd
- Any cycle can be written as a product of disjoint cycles and the order of a cycle is the lcm of its disjoint cycle lengths.
- S_n is not solvable for all $n \geq 5$, S_4 is solvable and S_3

Formula 1. *Automorphism Groups*

- $\text{Aut}(H \times K) \cong \text{Aut}(H) \times \text{Aut}(K)$ if $|H|$ and $|K|$ are coprime.
- $\text{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_{\varphi(m)}$ where φ is the Euler totient function,

$$\varphi(p_1^{e_1} \cdots p_n^{e_n}) = \varphi(p_1^{e_1}) \cdots \varphi(p_n^{e_n}) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_n^{e_n} - p_n^{e_n-1})$$

- $\text{Aut}(\mathbb{Z}_p^n) \cong GL_n(\mathbb{F}_p)$
- for $q = p^k$ $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$ (because each matrix is invertible so the columns must be linearly independnet, namely, q^n choices for first column, minus 0 vector; q^n choices for second column minus a linear combination of the first, so minus q; q^n choices for third minus q^2 for all the linear combinations of the previous two; etc.

- $|SL_n(\mathbb{F}_q)| = \frac{1}{q-1}|GL_n(\mathbb{F}_q)|$ because we quotient by the determinant.

Definition 2. *Group Action*

A group action of a group G on a set X defines a homomorphism $\varphi : G \to S_{|X|}$ defined by $\varphi(g) = \sigma_g$ where

$$\begin{aligned} \sigma_g : X &\to X \\ x &\mapsto g \cdot x \end{aligned}$$

***The two most useful group actions for qualifiying exams are:

- Conjugation action on a set of Sylow p-subgroups to help determine if they are normal
- Left multiplication on cosets of a subgroups to help determine if the subgroup is normal

Example 2.

Prove that there are no simple groups of order 600.

Let G be a group of order $600 = 10 \cdot 10 \cdot 6 = 2^3 \cdot 3 \cdot 5^2$.

By the Sylow Theorems, $n_5 \equiv 1 \mod 5$ and $n_5 | 2^3 \cdot 3$ so $n_5 = 1, 6$.

If G is simple, then $n_5 = 6$ and we can let G act on its Sylow 5 subgroups by conjugation (since Sylow 5-subgroups are conjugates).

This action defines a homomorphism $\varphi : G \to S_6$ where

$$\begin{aligned} \varphi(g) = \sigma_g : \mathrm{Syl}_5(G) &\to \mathrm{Syl}_5(G) \\ P_5 &\mapsto gP_5g^{-1} \end{aligned}$$

with P_5 a Sylow 5-subgroup of G.

Since kernels of homomorphisms are normal subgroups in the domain, if G is simple $\ker\varphi = \{e\}$. Namely, φ must be an embedding.

However, $|S_6| = 6! = 720$, and since $|G| = 600$ which does not divide 720, there cannot be any isomorphic copies of G inside S_6.

This is a contradiction and so $n_5 = 1$ and G cannot be simple.

Example 3.

For $n \geq 5$, there are no subgroups of S_n with $2 < [S_n : H] < n$.

Let H be a subgroup of S_n such that $2 < [S_n : H] = k < n$. Let S_n act on $X = S_n/H$ the set of left cosets of H by left-multiplication.

Then because $2 < |X| < n$, this induces a homomorphism from S_n to S_k where $k = |X|$.

Specifically, this defines a map

$$\begin{aligned} \varphi : S_n &\to S_{|X|} = S_k \\ a &\mapsto \sigma_a \end{aligned} \qquad \begin{aligned} \sigma_a : X &\to X \\ bH &\mapsto abH \end{aligned}$$

Now, we note that if $a \in \ker \varphi$, then $abH = bH$ for all $b \in S_n$ and so namely, $abh = bh'$ for $h, h' \in H$ so $a = bh'h^{-1}b^{-1} \in bHb^{-1}$ for all $b \in S_n$ and so namely, $\ker(\varphi) \subset H$.

Finally, we note that for $n \geq 5$, the only normal subgroups of S_n are the trivial subgroup, S_n itself, and A_n. Since $[S_n : A_n] = 2 < [S_n : H] < n$, $\ker(\varphi) \neq S_n$ and not A_n.

Namely, the kernel is trivial and so we have an embedding of S_n into a symmetric group of strictly smaller degree, which is of course, nonsense.

Thus, H cannot exist.

Galois and Field Theory

Definition 3. *Galois Field Extension*

If E/F is finite then E/F is Galois if E is the splitting field of a separable (all roots are distinct) polynomial $f \in F[x]$

Theorem 7. *Fundamental Theorem of Galois Theory*

If: E/F is Galois

Then: E is the splitting field of a separable polynomial $f(x) \in F[x]$ of degree n, and $G = \text{Gal}(E/F)$ is the set of automorphisms of E which fix F. Additionally,

- Every automorphism in G permutes the roots of each irreducible factor of f
- $|G| = [E : F] \leq n!$
- There is a 1-to-1 correspondence between subgroups of G and subfields of E containing F
- If H is a subgroup of G then there exists $K \subset E$ with $F \subset K$ so $H = \text{Gal}(E/K)$. Namely, $|H| = [E : K]$, $[G : H] = [K : F]$
- And H is normal in G if and only if K is Galois over F, and in this case $\text{Gal}(K/F) \cong G/H$

Theorem 8. *Eisenstein's Criterion*

If: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where a_i are an a UFD D, and there exists a prime element p such that $p \nmid |a_n$, $p|a_i$ for all $i \neq n$ and $p^2 \nmid |a_0$,

Then: $f(x)$ is irreducible in $D[x]$ and in $F[x]$ where F is the field of fractions of D.

Lemma 5. *Facts about Galois Extensions*

- If ξ_n is a primitive n^{th} root of unity, then $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$ where φ is the Euler totient function. Additionally, $\varphi(n)$ is the number of primitive n^{th} roots of unity.
- If ξ_n is a primitive n^{th} root of unity, then the splitting field K of $x^n - 1$ over $\mathbb{F}_q$ for $q = p^t$ some t, p prime, is a finite extension of $\mathbb{F}_q$. Namely, $K = \mathbb{F}_{q^k}$ some k. Now, to find k, we note that $\xi_n^{n+1} = \xi_n$ and $\xi_n^{q^k} = \xi_n$ because $\xi_n \in K$. Since $\xi_n^n = 1$, and n is minimal, we have that n divides $q^k - 1$. The smallest such k is the degree of the extension. Namely,
$$[\mathbb{F}_q(\xi_n) : \mathbb{F}_q] = k \qquad q^k \equiv 1 \mod n \text{ for } k \text{ minimal.}$$
- In fields of characteristic 0, irreducible implies separable

Example 4.

Let L be a Galois extension of a field F with $\text{Gal}(L/F) \cong D_{10}$, the dihedral group of order 10. How many subfields $F \subset M \subset L$ are there, what are their dimensions over F, and how many are Galois over F?

$|D_{10}| = 10 = 2 \cdot 5$. Thus, by Sylow, $n_5 \equiv 1 \mod 5$ and $n_5|2$ so $n_5 = 1$. Thus, D_{10} has one Sylow 5-subgroup which is normal. Since D_{10} is not abelian, $n_2 \neq 1$. Thus, $n_2 \equiv 1 \mod 2$ and $n_2|5$ so $n_2 = 5$.

There is the trivial subgroup $\{e\}$ which corresponds to the basefield F which is trivially Galois over itself.

There are 5 subgroups P_i $i = 1, ..., 5$ of order 2, which are not normal in G. Thus, there are 5 intermediate fields $F \subset M_i \subset L$ $i = 1, ..., 5$, such that $|P_i| = [L : M_i] = 2$ so $[M_i : F] = 5$ and M_i/F is not a Galois extension for $i = 1, ..., 5$.

There is 1 normal subgroup of order 5 Q. Thus, there is one intermediate field $F \subset K \subset L$ with $|Q| = 5 = [L : K]$ and $[K : F] = 2$ and K/F is a Galois extension.

Finally, there is the top field L which corresponds to $D_{10} = \text{Gal}(L/F)$ which is Galois over F and $[L : F] = 10$.

Definition 4. *Solvable Field Extension*

If E/F is a solvable extension if there exists a chain

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \alpha_2, ..., \alpha_n) = E$$

and for all i there exists an r_i such that $\alpha_{i+1}^{r_i} \in F(\alpha_1, ..., \alpha_i)$.

Theorem 9. *Solvable by Radicals*

If: E and F are characteristic 0 and E is the splitting field of $f(x) \in F[x]$ (f separable)

Then:

f is solvable by radicals $\iff$ E/F is a radical extension $\iff$ $\text{Gal}(E/F)$ is a solvable group

Theorem 10. *Finite Fields*

If: $\mathbb{F}_q$ is the field of q elements where p is prime

Then:

- $q = p^n$ for some prime p
- $\mathbb{F}_q$ is the splitting field (and set of roots) of $x^q - x$
- Any other field of q elements will be isomorphic to $\mathbb{F}_q$

Rings and Nullstellensatz

Theorem 11. *Isomorphism Theorems*

If R is a ring (or a module) and I, J are ideals (or submodules)

$$R/\ker(\varphi) \cong \mathfrak{Im}(\varphi) \qquad I+J/I \cong J/I\cap J \qquad (R/J)/(I/J) \cong R/I$$

Definition 5. *General Info about Ideals*

- I is an ideal of R if $x, y \in I$ implies $x - y \in I$, and if $rx \in I$ for all $r \in R$.
- $I + J = \{x + y \,|\, x \in I, y \in J\}$ is an ideal
- $IJ = \{\sum_{i=1}^{n} x_i y_i \,|\, x_i \in I, y_i \in J\}$ is an ideal
- Prime ideal P is such that $ab \in P$ implies $a \in P$ or $b \in P$ (if R is commutative then R/P is a domain)
- If R is commutative and M is a maximal ideal, then R/M is a field.
- $\sqrt{I} = \{r \in R \,|\,$ there exists m so $r^m \in I\}$.

Definition 6. *General Info about Rings*

- D is integrally closed if for every $k \in K$ the field of fractions of D, if k is algebraic over D (there exists $f \in D[x]$ so $f(k) = 0$) then $k \in D$
- R is Noetherian if it has ACC
- R is artinian if it has DCC

Theorem 12. *Cayley Hamilton*

Any matrix satisfies its characteristic polynomial.

Theorem 13. *Chinese Remainder Theorem*

If: $I_1, I_2, ..., I_n$ are pairwise coprime ($1 \in I_l + I_k$ for all $k \neq l$) 2-sided ideals of R

Then:

$$R \Big/ \bigcap_{k=1}^{n} I_k \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

***Note that if R is commutative then $\bigcap_{k=1}^{n} I_k = \prod_{k=1}^{n} I_k$.

Theorem 14. *Gauss' Lemma*

If: D is a domain, and K its field of fractions

Then: f is irreducible in $D[x] \iff f$ is irreducible in $K[x]$

Theorem 15. *Correspondence Theorem*

There is a 1-to-1 correspondence between:

$$\{\text{ maximal ideals of } R/I\} \iff \{\text{ maximal ideals of } R \text{ containing } I\}.$$

Example 5.

Prove that a power of the polynomial $(x+y)(x^2+y^4-2)$ belongs to the ideal (x^3+y^2, x^3+xy) in $\mathbb{C}[x,y]$.

It suffices to show that $(x+y)(x^2+y^4-2)$ is satisfied by all zeros in $V(x^3+y^2, x^3+xy)$ since by Nullstellenzatz, if $g(x,y)$ is a polynomial such that $g(a,b)=0$ for all $(a,b) \in V(I)$, then there exists an n such that $g^n(x,y) \in I$.

Let $g(x,y) = (x+y)(x^2+y^4-2)$. Clearly $(0,0) \in V(x^3+y^2, x^3+xy)$. If $x^3+y^2=0$ and $x^3+xy=0$ then $y^2-xy=0$, so $y(y-x)=0$. If $y=0$ then $x=0$, and if $y=x$, then $x^2(x+1)=0$, so $x=-1$.

Thus, the only elements of $V(x^3+y^2, x^3+xy)$ are $(0,0), (-1,-1)$.

Since $g(0,0)=0$ and $g(-1,-1)=0$, we have that there exists an n such that $g^n(x,y) \in (x^3+y^2, x^3+xy)$.

Theorem 16. *Nullstellensatz*

-
- Maximal ideals of $\mathbb{C}[x_1, ..., x_n]$ are of the form $(x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$ for $(a_1, ..., a_n) \in \mathbb{C}^n$
- $\sqrt{I}$ is the intersection of all maximal ideals of $\mathbb{C}[x_1, ..., x_n]$ containing I
- There is a 1-to-1 correspondence between $V(I)$ and $\sqrt{I}$
- $V(I) = \varnothing \iff 1 \in I$ (proper ideals have nonempty variety)
- If $g(a) = 0$ for all $a \in V(I) \iff g \in \sqrt{I}$ (there exists m such that $g^m \in I$)

Theorem 17. *Generalized Nullstellensatz*

If: k is a field and K is its algebraic closure,

Then:

- for $I \subset k[x_1, ..., x_n]$ and $V(I) \subset K^n$, $V(I) = \varnothing \iff 1 \in I$ (proper ideals have nonempty variety)
- If $g(a) = 0$ for all $a \in V(I) \subset K^n \iff$ there exists m such that $g^m \in I \subset k[x_1, ..., x_n]$

Theorem 18. *Hilbert Basis Theorem*

If: R is Noetherian

Then: $R[x]$ is Noetherian

***Note that R is Noetherian $\iff$ every ideal of R is finitely generated

Lemma 6. *Facts about Rings and Ideals*

- If R is a ring with 1, then for any ideal I there exists a maximal ideal M so $I \subset M$
- If D is a UFD, then $D[x]$ is UFD
- If F is a field, $F[x]$ is a PID
- UFDs are integerally closed in their field of fractions (by Gauss' Lemma)
- If R is Noetherian and I is a 2-sided ideal, then R/I is Noetherian
- If R is artinian, R/I is artinian for any ideal (including one-sided) of R.

Example 6.

> If F and $L = F[x_1, ..., x_n]/M$ are fields, then L is a finite field extension of F.

We proceed by induction on n. Basecase: let $L = F[a_1]$ be a field. Then for $f(a_1) \in L$ there exists $g(a_1) \in L$ such that $f(a_1)g(a_1) = 1 \in L$ and so a_1 satisfies $h(x) = f(x)g(x) - 1$. Namely, a_1 is algebraic over F and so L is a finite field extension of F.

Assume $L = F[a_1, ..., a_k]$ is a finite field extension of F for all $k \leq n$.

Then let $L = F[a_1, ..., a_n][a_{n+1}]$. Since L is a field, by the same reasoning as the basecase, L is algebraic over $F[a_1, ..., a_n]$. However, by the inductive hypothesis, $F[a_1, ..., a_n]$ is a finite field extension of F and so $[L : F] = [L : F[a_1, ..., a_n]][F[a_1, ..., a_n] : F] < \infty$.

Example 7.

> If L is a finite field extension of F, then there exists only finitely many embeddings of L into K the algebraic closure of F.

We proceed by induction. Basecase: let $L = F(a_1)$ be a finite extension of F. Because a_1 is algebraic over F, it has minimal (irreducible) polynomial

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in F[x].$$

Now, if $\varphi : L \hookrightarrow K$, because $\varphi(1) = 1$, φ is F-linear and so

$$\varphi(f(a_1)) = \varphi(a_1)^n + \alpha_{n-1}\varphi(a_1)^{n-1} + \cdots + \alpha_1\varphi(a_1) + \alpha_0 = 0$$

so φ permutes the roots of $f(x)$. Note that K is the algebraic closure of F and so contains all such roots.

Thus, there are only finitely many possible choices of φ since there are only finitely many roots of $f(x)$.

Now, assume there are only finitely many injections of $L = F(a_1, ..., a_k)$ to K for $k \leq n$.

Then we examine $L = F(a_1, ..., a_n, a_{n+1}) = F(a_1, ..., a_n)(a_{n+1})$. Then there are only finitely many $F(a_1, ..., a_n)$-linear injections from $L \hookrightarrow K$ by the same reasoning as the basecase, and by the induction hypothesis, only finitely many F-linear injections from $F(a_1, ..., a_n) \hookrightarrow K$.

Since any injection $L \hookrightarrow K$ will be defined by where it sends the a_i, and since there are only finitely many choices for where to send $a_1, ..., a_n$ and only finitely many choices for where to send a_{n+1}, we have only finitely many possible injections of L into K.

Modules and Algebras

Definition 7. *Module*

A module (left or right, rarely 2-sided) over a ring is the generalization of a vector space over a field.

There is no notion of multiplication in a module other than multiplication by scalars in the base ring.

Theorem 19. *Classification of Finitely Generated Modules*

If: R is a PID and M is finitely generated over R

Then: $M \cong R^n \oplus T(M)$ where $R^n \cong R \oplus R \oplus \cdots \oplus R$ is the free part of M and $T(M) = \{m \in M \mid \text{ there exists } 0 \neq r \in R \text{ so } rm = 0\}$ is the torsion submodule of M.

*** We can write $T(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_n)$ for

$$(a_1) \supset (a_2) \supset \cdots \supset (a_n)$$

all ideals.

Definition 8. *Projective Module*

An R-module P is projective if there exists an R-module N so $P \oplus N$ is free (so for some n, $P \oplus N \cong R^n$).

Lemma 7. *Facts about Modules*

- M is simple if $M \cong R/M$ for some maximal (left or right) ideal M.
- If P is projective and $0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$ is a short exact sequence, then $M \cong P \oplus N$

Lemma 8. *Facts about Jacobson Radical*

- $J(R)$ is the intersection of all maximal (right) ideals of R
- $J(R)$ is quasi-regular, so for all $r \in J(R)$, $1 - r$ is invertible in R.
- If R is artinian, then $J(R)$ is nilpotent
- If R is commutative, then $J(R)$ contains all the nilpotent elements of R.
- $J(R/J(R)) = 0$

Theorem 20. *Schur's Lemma*

If: M and N are simple R-modules

Then: any module homomorphism $f : M \to N$ is either identically 0 or an isomorphism.

Definition 9. *Algebra over a field*

An algebra over a field is a vector space with a multiplication action which has F in its center (it is a ring and a vector space at the same time).

Lemma 9. *Fact about Algebras*

If A is a finite dimensional F-algebra for F a field, then A is artinian and Noetherian

Theorem 21. *Frobenius Theorem*

If: D is a division ring which is finite dimensional over $\mathbb{R}$

Then: $D \cong \mathbb{R}, \mathbb{C}, \mathbb{H}$.

Theorem 22. *Artin-Wedderburn*

TFAE:

- R is artinian and $J(R) = 0$
- R is semi-simple (R is a finite direct sum of minimal left ideals)
- $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$ for D_i division rings over R.

***Note that a finite division ring is a finite field by Wedderburn's Little Theorem

Definition 10. *Group Algebra*

If G is a finite group and F is a field with $\text{char}(F)$ coprime to $|G|$, then $F[G]$ is the set of sums of elements of the form ag where $a \in F$ and $g \in G$.

Lemma 10. *Facts about Group Algebras*

- Maschke's Theorem: $F[G]$ as from the previous definition is semi-simple
- If $F[G] = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, then D_i are division rings over F.
- By Frobenius, $n_i||G|$ for all i and $|G| = \sum_{i=1}^{n} n_i^2$

Example 8.

Determine up to isomorphism the algebra structure of $\mathbb{C}[G]$ where $G = S_3$ is the symmetric group of degree 3.

By Artin Wedderburn, $\mathbb{C}[S_3]$ is semi-simple of dimension 6 so

$$\mathbb{C}[S_3] \cong \mathbb{C}^a \oplus (M_2(D))^b$$

where D is a division ring over $\mathbb{C}$.

Note that $M_n(D)$ cannot appear for $n > 2$ since the dimension of the algebra is 6 and $M_3(D)$ has dimension $3^2 = 9$. For the same reason, there can be only one copy of $M_2(D)$. Namely, $b = 0, 1$.

Furthermore, by Frobenius, the only division ring over $\mathbb{C}$ is $\mathbb{H}$, and since $\mathbb{C} \subset Z(\mathbb{C}[S_3])$ is contained in the center of the algebra (definition of algebra), we have that $\mathbb{H}$ cannot appear in the decomposition. Also, $D = \mathbb{C}$ since any central division ring over an algebraically closed field is the base field.

Finally, since S_3 is non commutative, $b = 1$ and so

$$\mathbb{C}[S_3] \cong \mathbb{C}^2 \oplus M_2(D).$$

Definition 11. *Tensor Product*

Tensor product of R-modules is an R-modules with a universal property, that for all abelian groups G, and homomorphism $f : A \times B \to G$, and $i : A \times B \to A \otimes_R B$ defined by $i(a, b) = a \otimes b$, there exists a unique g such that the diagram commutes, namely $f = g \circ i$.

$$\begin{array}{ccc} A \times B & \xrightarrow{f} & G \\ {\scriptstyle i}\downarrow & \swarrow{\scriptstyle g} & \\ A \times_R B & & \end{array}$$

Facts of tensor sums:

- If $r \in R$, $r(a \otimes b) = ra \otimes b = a \otimes rb$.
- $(a + b) \otimes c = a \otimes c + b \otimes c$.
- $0 \otimes b = a \otimes 0 = 0$.

Lemma 11. *Facts about Tensor Products*

- $R \otimes_R M \cong M \cong M \otimes_R R$
- $$(M \oplus N) \otimes_R Q \cong (M \otimes_R Q) \oplus (N \otimes_R Q),$$
  $$Q \otimes_R (M \oplus N) \cong (Q \otimes_R M) \oplus (Q \otimes_R N)$$
- Tensor is right exact, namely given a sequence

  $$0 \longrightarrow N \longrightarrow M \longrightarrow Q \longrightarrow 0$$

  we have that

  $$N \otimes_R P \longrightarrow M \otimes_R P \longrightarrow Q \otimes_R P \longrightarrow 0$$