Math 6310 Algebra I

Taught by Marcelo Aguiar
Notes by Aaron Lou

Fall 2019

Contents

1 Aug 29

1.1 Basic Notions

Def.

- ***Groups*** *are sets with binary operation closed, associative, inverse, identity.*
- ***Subgroup*** $H \leq G$ *contains unit, inverse, and closed.*
- ***Normal subgroup*** $N \trianglelefteq G : gNg^{-1} = N$.
- *We have* ***quotient group*** G/N
- ***Homomorphisms*** $\varphi : G_1 \to G_2$ *s.t.* $\varphi(a+b) = \varphi(a)+\varphi(b)$. *We have* $\ker(\varphi) \trianglelefteq G_1, \operatorname{im}(\varphi) \leq G_2$.
- ***Injectivity*** *of* φ *means* $\ker(\varphi) = \{1\}$,***surjective*** *means that* $\operatorname{im}(\varphi) = G_2$, ***bijective*** *means isomorphism and both and inverse is homomorphism.*

1.2 Isomorphism Laws

Prop 1.1 (First Isomorphism Law)**.**

(i) Let $N \trianglelefteq G$ *and* $\pi : G \to G/N$ *be the canonical projection* $\pi(g) = gN$. *Then* π *is a surjective homomorphism and* $\ker(\pi) = N$.

(ii) Let $\varphi : G \to Q$ *be a surjective homomorphism with* $\ker(\varphi) = N$. *Then* $\widehat{\varphi} : G/N \to Q$ *given by* $\widehat{\varphi}(gN) = \varphi(g)$ *is a well define isomorphism and the following diagram commutes*

$$\begin{tikzcd} N \arrow[r, hook] & G \arrow[r, "\pi"] \arrow[dr, two heads, "\varphi"] & G/N \arrow[d, "\widehat{\varphi}"] \\ & & Q \end{tikzcd}$$

Prop 1.2 (Universal Property of Quotient UPQ)**.** *Let* $N \trianglelefteq G$ *and* $\varphi : G \to H$ *be a homomorphism with* $N \leq \ker(\varphi)$ *then there is a homomorphism* $\widehat{\varphi} : G/N \to H$ *s.t.* $\varphi = \widehat{\varphi} \circ \pi$.

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, twoheadrightarrow, "\pi"] & H \\ G/N \arrow[ur, "\widehat{\varphi}"'] & \end{tikzcd}$$

Moreover, $\ker(\widehat{\varphi}) = \ker(\varphi)/N$ $\operatorname{im}(\widehat{\varphi}) = \operatorname{im}(\varphi)$

Def. *Given subsets X, Y of G, $XY = \{xy, x \in X, y \in Y\}$.*

Remark. *Even if $X, Y \leq G$, $XY \leq G$ is not true necessarily.*

Def. $N_G(X) = \{g \in G : gXg^{-1} = X\}$. *$Y$ **normalizes** X if $Y \subseteq N_G(X)$.*

Remark. *$Y \leq G$, then: Y normalizes $X \iff yXy^{-1} \subseteq X\ \forall y \in Y$.*

Proof. $(\rightarrow)$ is trivial. $(\leftarrow)$ is that $y^{-1}Xy \subseteq X \implies yy^{-1}Xyy^{-1} \subseteq yXy^{-1}$. $\square$

Remark. *$N_G(X) \leq G$ for all $X \subseteq G$.*

Prop 1.3 (Second Isomorphism Law)**.** *Let $N, H \leq G$ s.t. H normalizes N.*

(1) $NH = HN \leq G$.

(2) $N \trianglelefteq NH$ *and* $N \cap H \trianglelefteq H$.

(3) $NH/N \cong H/N \cap H$.

$$\begin{array}{ccccc} & & G & & \\ & & | & & \\ & & NH & & \\ & /\!\!/ & & \backslash & \\ N & & & & H \\ & \backslash & & /\!\!/ & \\ & & N \cap H & & \end{array}$$

Proof.

(1) $hNh^{-1} = N \rightarrow hN = Nh$. $n_1h_1n_2h_1 = n_1n_3h_3h_2 \in NH$. $(nh)^{-1} = hn \in HN = NH$.

(2) H normalizes N by hypothesis. N normalizes N. $N \trianglelefteq NH$ as $nh \in NH$ and $(nh)N(nh)^{-1} = nhNh^{-1}n^{-1} \subset nNn^{-1} \subseteq N$. For $N \cap H \trianglelefteq H$, note that $h \in H, x \in N \cap H$ then $hxh^{-1} \in H$ and $hxh^{-1} \in X$ so $h(N \cap H)h^{-1} \subseteq N \cap H$ and so $N \cap H$ is normal in H.

(3)

$$\begin{tikzcd} N \cap H \arrow[r, hook] & H \arrow[r, two heads] \arrow[d, hook] \arrow[dr, "\varphi"] & H/N \cap H \\ N \arrow[r, hook, two heads] & NH \arrow[r, two heads, "\pi"] & NH/N \end{tikzcd}$$

Let $\varphi : H \to NH/N$ be the restriction of $\pi : NH \to NH/N$ to H. Then $\ker(\varphi) = N \cap H$ and φ is surjective as $\overline{nh} = \overline{n}\overline{h} = \overline{h} = \varphi(h)$. Apply first isomorphism to φ so we have that $H/N \cap H \cong NH/N$ as $N \cap H$ is kernel, H is domain, image is NH/N.

$\square$

Prop 1.4 (Third Isomorphism Law)**.** *Let $N, K \trianglelefteq G$ with $N \subseteq K$.*

(1) $K/N \trianglelefteq G/N$.

(2) $\frac{G/N}{K/N} \cong G/K$.

$$\begin{tikzcd} G \arrow[d, dash] & G/N \arrow[d, dash] \\ K \arrow[d, dash] & K/N \arrow[d, dash] \\ N & \{1\} \end{tikzcd}$$

Proof. Consider $\pi : G \to G/K$, then $N \subseteq K = \ker(\pi)$. By UPQ there is a homomorphism $\widehat{\pi} : G/N \to G/K$ and $\ker(\widehat{\pi}) = G/N$ and $\mathrm{im}(\widehat{\widehat{\pi}}) = G/K$. By first isomorphism theorem, we are done.

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d] & G/K \\ G/N \arrow[ur, "\widehat{\pi}"] & \end{tikzcd}$$

$\square$

Prop 1.5 (Fourth Isomorphism Law). *Let $N \trianglelefteq G$.*

(1) *If $N \subseteq H \leq G \implies H/N \leq G/N$.*

(2) *If $Q \leq G/N$ then there exists a unique H s.t. $N \subseteq H \leq G$ and $Q = H/N$. There is a bijective correspondence between subgroups of G/N and intermediate subgroup of G.*

(3) *This correspondence preserves inclusion and normality: $H_1 \leq H_2 \iff H_1/N \leq H_2/N$ and $H_1 \trianglelefteq H_2 \iff H_1/N \trianglelefteq H_2/N$.*

1.3 Modularity

Let $X, Y, Z \leq G$. We ask if $X \cap YZ = (X \cap Y)(X \cap Z)$ (distributivity). This doesn't hold. If $G = \mathbb{Z}^2$ as if Y, Z are the axes and X a diagonal line, then $X \cap YZ = X \neq (X \cap Y)(X \cap Z) = \{1\}$.

Prop 1.6 (Dedekind's modularity law). *Let $X, Y, Z \leq G$ s.t. $Z \subseteq X$. Then $X \cap YZ = (X \cap Y)Z$. Or we have $X \cap YZ = XZ \cap YZ = (X \cap Y)Z = (X \cap Y)(X \cap Z)$.*

Proof. $(\supseteq)$: $X \cap Y \subseteq X, Z \subseteq X \implies (X \cap Y)Z \subseteq X$. Furthermore, $X \cap Y \subseteq Y, Z \subseteq Z \implies (X \cap Y)Z \subseteq YZ$ so this proves this direction.

$(\subseteq)$: $x = yz \in X \cap YZ$. $y = xz^{-1} \in X \implies y \in X$. So, $x = yz \in (X \cap Y)Z$. $\square$

Remark. *$\mathcal{L}(G) = \{H \subseteq G : H \leq G\}$. This is a poset by $\subseteq$. It's a lattice as well. The meet is $H_1 \cap H_2$ and the join is $\langle H_1 \cup H_2 \rangle$.*

$\mathcal{N}(G) = \{N \trianglelefteq G\}$. $N_1 \wedge N_2 = N_1 \cap N_2$, $N_1 \vee N_2 = N_1 N_2$. It is a modular lattice.

2 September 3

2.1 Butterfly Lemma

The butterfly law comes from trying to embed a chain of subgroups $B_1 \leq B$ into $A_1 \leq A$. We want to use the NH diamond to get $A_1 \leq A_1(A \cap B_1) \leq A_1(A \cap B) \leq A$. By Dedekind's Modularity Law, our ordering is unaffected as $A_1(A \cap B) = A \cap A_1 B$ so our intersection and multiplication order doesn't matter.

Prop 2.1 (Butterfly, Zausenhaus). *Let $A_1 \trianglelefteq A \leq G, B_1 \trianglelefteq B \leq G$. Then*

(1) $A_1(A \cap B_1) \trianglelefteq A_1(A \cap B) \leq G$. $(A_1 \cap B)B_1 \trianglelefteq (A \cap B)B_1 \leq G$.

(2) $\frac{A_1(A \cap B)}{A_1(A \cap B_1)} \cong \frac{(A \cap B)B_1}{(A_1 \cap B)B_1}$.

Proof.

(1) A normalizes A_1 so $A \cap b$ normalizes A_1. Therefore, $A_1(A \cap B) \leq G$ and similarly for others. A_1 normalizes $A_1(A \cap B_1)$ as A_1 is a subgroup of $A_1(A \cap B_1)$. $A \cap B$ normalizes $A_1(A \cap B_1)$ as $A \cap B$ normalizes A_1 and $A \cap B_1$.

(2) We build the butterfly diagram

$$\begin{tikzcd}
A \arrow[d, dash] & & B \arrow[d, dash] \\
A_1(A \cap B) \arrow[dr, dash] \arrow[dd, dash] & & (A \cap B)B_1 \arrow[dl, dash] \arrow[dd, dash] \\
& A \cap B \arrow[dd, dash] & \\
A_1(A \cap B_1) \arrow[dr, dash] \arrow[dd, dash] & & (A_1 \cap B)B_1 \arrow[dl, dash] \arrow[dd, dash] \\
& (A_1 \cap B)(A \cap B_1) \arrow[ddl, dash] \arrow[ddr, dash] & \\
A_1 \arrow[d, dash] & & B_1 \arrow[d, dash] \\
A_1 \cap B & & A \cap B_1
\end{tikzcd}$$

The top left and right parallelograms are NH diamonds. Then apply $2nd$ isomorphism law to both and deduce the desired result. To show this, note that $A_1(A \cap B_1)(A \cap B) = A_1(A \cap B)$. Note that $A_1(A \cap B) \cap (A \cap B) = (A_1 \cap A \cap B)(A \cap B_1 \cap A \cap B) = (A_1 \cap B)(A \cap B_1)$ as $A \cap B$ normalizes $A_1(A \cap B_1)$.

∎

2.2 Series

Def. *Let G be a group. A **series** is a finite sequence of subgroups, each contained in the preceding and ranging from G to $\{1\}$.*

$$G = G_0 \geq G_1 \cdots \geq G_m = \{1\}$$

*The **length** is m. It is is proper if $G_i \neq G_{i-1}$. It is **subnormal** if $G_i \trianglelefteq G_{i-1}$ and normal if $G_i \trianglelefteq G\ \forall i$. A second series of G is a **refinement** if it contains all elements of the first series but more. In a subnormal series, the G_{i-1}/G_i are **slices**. Note that the group is **proper** if all slices are nontrivial. Two subnormal series are **equivalent** if their nontrivial slices are isomorphic, possibly in different order, with same multiplicity.*

Theorem 2.1 (Schreir's Refinement)**.** *Let $\{G_i\}_{0\leq i\leq n}$ and $\{H_j\}_{0\leq j\leq m}$ be two subnormal series of G. There exists refinements $\{G'_i\}_{0\leq i\leq mn}$ and $\{H'_j\}_{0\leq j\leq m'}$ that are equivalent.*

Proof. For each i and j, insert H_j into $G_{i+1} \leq G_i$ (as in butterfly lemma) $G_{ij} = G_{i+1}(G_i \cap H_j)$. We have that

$$G_i \geq G_{i,0} \geq \ldots G_{i,m} \geq G_{i+1}$$

Note that $G_i = G_{i,0}, G_{i,m} = G_{i+1}$. By BL it is subnormal. Piecing these chains together with i to obtain a subnormal refinement of $\{G_i\}$ and do the same with $\{H_j\}$. These new chains are equivalent as $G_{i,j}/G_{i,j+1} \cong H_{j,i}/H_{j,i+1}$ by the BL. □

2.3 Simple Groups

Def. *A group G is **simple** if the only normal subgroups are G and 1 and is nontrivial.*

Def. *A **composition series** is a subnormal series for which all slices are simple.*

Ex.

- $D_n = \{\rho, \sigma : \rho^m = \sigma^2 = 1, \sigma\rho = \rho^{-1}\sigma\}$*. The elements $\sigma\rho^i$ and ρ^i and there are $2n$ elements. An example is $D_n \triangleright \langle\rho\rangle \triangleright \{1\}$ with slices $\mathbb{Z}_2, \mathbb{Z}_n$.*
- $\mathbb{Z}_6 \triangleright \langle\overline{2}\rangle \triangleright \langle\overline{0}\rangle$ *with slices $\mathbb{Z}_2, \mathbb{Z}_3$.*
- $\mathbb{Z}_6 \triangleright \langle\overline{3}\rangle \triangleright \langle\overline{0}\rangle$ *with slices $\mathbb{Z}_2, \mathbb{Z}_3$.*
- $GL(n, \mathbb{F}) \triangleright SL(n, \mathbb{F}) \triangleright \mu_n(\mathbb{F}) \triangleright \{1\}$ *as SL is kernel of determinant. Slice is $\mathbb{F}^x$, $PSL(n, \mathbb{F})$, μ_m.*

3 September 5

3.1 Simple Groups Cont

Ex.

- *A group is simple and abelian iff it is cyclic with prime order.*
- $A_n = \{\sigma \in S_n : \sigma \text{is even}\}$ *is simple for* $n \neq 1, 2, 4$. A_4 *is not simple as it contains* $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. *In particular* $V_4 = \{id, (12)(34), (13)(24), (14)(23)\}$ *and this is normal.*
- $PSL(n, \mathbb{F}_q)$ *is simple when* $n = 2, q = 2, 3$ *or* $n = 1$ *(will show in a couple of weeks).*

Def. *A* ***composition series*** *of a group if it is a proper subnormal series that has no proper refinements. Equivalently, all slices are simple groups. The slices are called the* ***composition factors****.*

Ex.

- $\mathbb{Z}$ *doesn't have a composition series, as everything must be of the form* $\mathbb{Z} \rhd p_1\mathbb{Z} \rhd p_1p_2\mathbb{Z} \dots$ *and this never reaches* 0.
- $\mathbb{Z}_6 \rhd \langle \overline{2} \rangle \rhd \{\overline{0}\}$ *and* $\mathbb{Z}_6 \rhd \{\overline{3}\} \rhd \{\overline{0}\}$ *are two composition series.*
- *Any finite group has a composition series. Proof by strong induction.*

Theorem 3.1 (Jordan-Holder Thm)**.** *Let* G *be a group with a composition series. Any two composition series of* G *are equivalent.*

Proof. Any two composition series $\{G_i\}$ and $\{H_j\}$ have subnormal refinements that are equivalent by Schreir's. They are the same (added a bunch of 1 slices) and since the two composition series are proper they are equivalent as their refinements are equivalent. □

Remark. *The composition factors of* G *depend on* G *and not on the selection of composition series. However, the same doesn't hold the other way around: composition series factors may define two groups.*

Ex. *For* $n > 4$, $S_n \rhd A_n \rhd \{id\}$ *has slices* $\mathbb{Z}_2, A_n$ *and is a composition series as both are simple.*

3.2 Solvable Groups

Def. *A group is **solvable** if it admits a subnormal series with all slices abelian.*

Ex.

- *Any abelian group is solvable.*
- $D_n \triangleright \langle \sigma \rangle \triangleright \{1\}$.

Prop 3.1. *Let G be solvable and $H \leq G$. Then*

- *H is solvable*
- *iff $H \trianglelefteq G$, G/H is solvable.*

Proof. Same is true for abelian groups. Pick a subnormal series for G with abelian slices and intersect on H and project to G/H. □

Prop 3.2. *Let $N \trianglelefteq G$. Then G is solvable iff $N, G/N$ solvable.*

Proof. ($\Rightarrow$). Previous prop

($\Leftarrow$) pick series for $N, G/N$ and lift the former to subgroup between N and G using 4th isomorphism law. □

Prop 3.3. *Let G be solvable. Then every subnormal series has a refinement with abelian slices.*

Proof. Schreir's on both. □

Prop 3.4. *Let G be a group with composition series. The following are equivalent*

(i) G is solvable.

(ii) All composition factors are abelian.

(iii) All composition factors are cyclic of prime order.

Proof. $(i) \to (ii)$. Apply previous prop to given comp series.
$(ii) \to (iii)$. Simple Abelian groups are cyclic of prime order.
$(iii) \to (i)$ by definition. □

Ex. *S_n is not solvable for $n > 4$ as A_n is not abelian.*

3.3 The Derived Series

Def. *The* ***commutator*** *of $g, h \in G$ is $[g, h] = ghg^{-1}h^{-1}$. The* ***commutator*** *of $H, K \leq G$ is $[H, K] = \bigcap_{S \leq G, \{[h,k]\} \subseteq S} S$.*

Lemma.

- *$[G, G] = \{1\}$ iff and only iff G is abelian.*
- *Let $N \leq G$. Then $[G, G] \subseteq N \iff N \trianglelefteq G$ and G/N is abelian.*

Proof. Homework exercise (2-11). □

Def. *The derived subgroup of G is $G^{(1)} = [G, G]$ and $G^{(i)} = (G^{(i-1)})^{(1)}$. Note that $G^{(i)} \trianglelefteq G^{(i-1)}$ and $G^{(i-1)}/G^{(i)}$ are abelian, but it may not terminate. This is the* ***derived series****.*

Prop 3.5. *Each $G^{(i)}$ is characteristic in G. Recall that characteristic means that H is mapped to a subgroup of H for any automorphism of G.*

Proof. $\sigma([g, h]) = [\sigma(g), \sigma(h)]$. Use the fact that being characteristic is transitive. □

Prop 3.6. *Let G be a group. The following are equivalent*

(i) G is solvable.

(ii) $\exists m \geq 0$ s.t. $G^{(m)} = \{1\}$.

(iii) G has a normal series with abelian slices.

Proof. $(ii) \to (iii) \to (i)$ is obvious as we use the derived series and if normal series are subnormal. To prove $(i) \to (ii)$, we note that in a derived series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$ then we can use our lemma to show that $G^{(1)} \leq G_1, G_1^{(1)} \leq G_2$ etc. and therefore we have by induction $G^{(i)} \leq G_i$ which proves (ii). □

3.4 Nilpotent Groups

Def. *A group G is* ***nilpotent*** *if it admits a normal series $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n \trianglerighteq \{1\}$ s.t. $G_{i-1}/G_i \subseteq Z(G/G_i)$ for all $i = 1, \ldots, m$.*

Ex. *Abelian $\implies$ nilpotent $\implies$ solvable.*

Remark. *G nilpotent implies that $Z(G) \neq \{1\}$.*

Prop 3.7.

1. *G nilpotent, $H \leq G$ means H nilpotent.*
2. *G nilpotent, $N \trianglelefteq G$ then G/N is nilpotent.*
3. *$N \leq Z(G)$ and G/N nilpotent implies that G is nilpotent.*

4 September 10

4.1 Nilpotent Groups Revisited

Prop 4.1.

1. *G nilpotent and $H \leq G \implies H$ nilpotent.*
2. *G nilpotent and $N \trianglelefteq G$ implies that G/N nilpotent.*
3. *$N \leq Z(G)$ and G/N is nilpotent means that G is nilpotent.*

Proof. HW2, Exercise 9. □

Ex. *HW2, Ex 10. D_n is nilpotent iff $n = 2^\alpha$ for some α.*

4.2 The Lower Central Series

Def. *Define subgroups of G as follows.*

$$G^{[0]} = G, G^{[i]} = [G, G^{[i-1]}]$$

*$G = G^{[0]} \trianglerighteq G^{[1]} \cdots \trianglerighteq$ is the **lower central series** of G.*

Prop 4.2.

1. *$G^{[i]}$ is characteristic in G for each i.*
2. *$G = G^{[0]} \trianglerighteq G^{[1]} \dots$ is well defined*
3. *$G^{[i-1]}/G^{[i]} \subseteq Z(G/G^{[i]})$.*

Prop 4.3. *G is nilpotent iff $\exists n \geq 0$ s.t. $G^{[n]} = \{1\}$.*

4.3 Group Actions

Def. *Let G be a group and Ω a set. The **left action** of G on Ω is a function $G \times \Omega \to \Omega$ with $(g, \alpha) \to g \cdot \alpha$ s.t. $1 \cdot \alpha = \alpha$ and $g \cdot (h \cdot \alpha) = gh \cdot \alpha$. The **right action** is the same thing.*

*For $\alpha, \beta \in \Omega$, $\alpha \sim \beta$ if $g \cdot \alpha = \beta$ for some $g \in G$. $\sim$ is an equivalence relation and the classes are called the **orbits** of the action. It is denoted $O_G(\alpha) = \{g \cdot \alpha | g \in G\}$.*

*The **stabilizer** of an element $\alpha \in \Omega$ is given by $S_G(\alpha) = \{g \in G | g \cdot \alpha = \alpha\}$. $O_G(\alpha) \subseteq \Omega$ and $S_G(\alpha) \leq G$.*

Def. *The action is* ***transitive*** *when there is only one orbit or* $g \cdot \alpha = \beta$ *for all* α, β.

Ex.

1. $G = (\mathbb{R}, +)$, $\Omega = \mathbb{C}$. $x \cdot z = e^{ix}z$. *The orbits are circles of varying radius and the stabilizer is* $S_G(0) = \mathbb{R}$ *and* $S_G(z) = 2\pi\mathbb{Z}$.

2. G *be any group,* $\Omega = G$ *then the* ***action of conjugation*** *is given by* $h \to ghg^{-1}$. $S_G(h)$ *is the centralizer of* h *in* G *and* $O_G(h)$ *is the conjugacy class of* h *in* G.

3. S_n *acts on* $\{1, 2, \ldots, n\}$ *by* $\sigma \cdot i = \sigma(u)$. *This action is transitive because there is always a permutation sending* i *to* j.

Prop 4.4. *Let* G *act on* Ω, $\alpha \in \Omega$. *Then*

1. $S_G(\alpha) \leq G$.

2. $|G/S_G(\alpha)| = |O_G(\alpha)|$

3. $\alpha \sim \beta$ *then there is a* $g \in G$ *s.t.* $gS_G(\beta)g^{-1} = S_G(\alpha)$.

Ex. *Let* $k \leq n$ *be nonnegative integers,* $\mathbb{P}_k(n) = \{A \subseteq \{1, 2, \ldots, n\} | |A| = k\}$. S_n *acts on* $\mathbb{P}_k(n)$ *by* $\sigma \cdot A = \sigma(A)$. *Let* $A_0 = \{1, 2, \ldots, k\} \in \mathbb{P}_k(n)$. *Then* $O_{S_n}(A_0) = \mathbb{P}_k(n)$ *so the action is transitive.* $S_{S_n}(A_0) \cong S_k \times S_{n-k}$ *under isomorphism* $\sigma \to (\sigma|_{A_0}, \sigma|_{A_0^c})$. *Therefore*

$$|\mathbb{P}_k(n)| = |S_n/S_{S_n}(A_0)| = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Prop 4.5. *Let* G *act on finite* Ω *and all stabilizers are trivial. Then the number of orbits is* $|\Omega|/|G|$. G *is finite and* $|G| \mid |\Omega|$.

Proof. $|O_G(\alpha)| = |G/S_G(\alpha)| = |G|$. We see that $\Omega = \bigsqcup_{i=1}^k O_G(\alpha_i)$ so $|\Omega| = \sum_{i=1}^k |O_G(\alpha_i)| = k|G|$. $\square$

Ex. *Let* $H \leq G$ *with finite* g. $(g, h) \to gh$ *is a right action of* H *on* G. $O_H(g) = gH$ *so the orbits are the* H*-cosets.* $|G : H| = |G/H|$. $S_H(g) = \{1\}$ *so the stabilizers are trivial. By proposition we get Lagrange's thm* $|G/H| = |G|/|H|$.

Ex. *Let* $\mathbb{P}^n(\mathbb{F})$ *be the* n*-dimensional projective space over a field* $\mathbb{F}$. *This is the lines through the origin in* $\mathbb{F}^{n+1}$. *The slopes cover the line, with a point at infinity. HW3 exercise 3 will derive*

$$|\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + \cdots + q^n$$

Def. *For G acting on Ω, Ω^G is the set of fixed points $\{\alpha \in \Omega : g \cdot \alpha = \alpha \forall g \in G\}$.*

Theorem 4.1 (Fixed point lemma)**.** *Let G act on finite Ω. Suppose there is a p s.t. $p|[G : H]$ for all $H < G$. Then $|\Omega^G| \equiv |\Omega| \pmod p$.*

Proof. Examine orbits $O_G(\alpha_1), \ldots, O_G(\alpha_i), O_G(\alpha_{i+1}), \ldots, O_G(\alpha_k)$, where $O_G(\alpha_i)$ and before are trivial and rest are not. Then $|\Omega| = |\Omega^G| + |G/S_G(\alpha_{i+1})| + \cdots + |G/S_G(\alpha_k)|$. Clearly the other stabilizer terms are proper, as their respective orbits are nontrivial and we have $|\Omega| \equiv |\Omega^G| \pmod p$. □

4.4 Actions and groups of permutations

If G acts on Ω from the left. If we define $\varphi_g(\alpha) = g \cdot \alpha$ then $(\varphi_g)^{-1} = \varphi_{g^{-1}}$. If $S(\Omega)$ is the group of permutations of Ω then $\varphi : g \to \varphi_g$ is a group homomorphism and we can construct φ_g from φ and similarly the other way around.

Remark. *Right actions give us an anti-homomorphism ie reverse order.*

Def. *Let G act on Ω and let $\varphi : G \to S(\Omega)$ be the group morphism. $\ker \varphi$ is the* ***kernel of the action****. The action is* ***faithful*** *if $\ker \varphi$ is trivial, or φ is injective.*

Remark. *$g \in \ker \varphi \iff \varphi_g = \mathrm{id}_\Omega \iff g \cdot \alpha = \alpha \ \forall \alpha$ or if $g \in S_G(\alpha)$ for all α. We have that*

$$\ker \varphi = \bigcap_{\alpha \in \Omega} S_G(\alpha)$$

Ex.

1. *G acts on itself by conjugation. Then $S_G(h)$ is the centralizer of h in G and $\ker \varphi = \bigcap_{h \in G} S_G(h) = Z(G)$.*

2. *S_n acts on $\{1, \ldots, n\}$. $S_G(i) = \{\sigma \in S_n | \sigma(i) = i\} \equiv S_{n-1}$. however, $\ker \varphi = \{\sigma \in S_n | \sigma(i) = i \ \forall i\} = \{\mathrm{id}\}$. $\varphi : S_n \to S_n$ is the identity.*

3. *G acts on itself by left translations $g \cdot h = gh$. $S_G(h) = \{1\}$ so the action is faithful. $\varphi : G \to S(G)$ is injective. This is* ***Cayley's Thm*** *that any group is isomorphic to a subgroup of a permutation group.*

5 September 12

5.1 Applications to Existence of Normal Subgroups

If we recall an action of G on X, then the kernel is the intersection of all stabilizers of x.

Prop 5.1 (n! lemma)**.** *Let $H \leq G$ and $|G/H| = n$ (G/H is a set). Then there exists a $N \trianglelefteq G$ s.t. $N \subseteq H$ and $|G/N|$ divides $n!$.*

Proof. Let $\Omega = G/H = \{gH\}$. Define $g \cdot xH = gxH$. This is a left action of G on Ω. Let $N = \ker(\varphi)$ where φ is associated morphism. The kernel is the intersection of stabilizers, and In particular $N \subseteq S_G(H) = H$ (note that H is $1H$ on the LHS).

By first isomorphism law, $G/N \hookrightarrow S(\Omega) \implies |G/N| \leq |S(\Omega)| = n!$. □

Corrollary. *Let G be finite and p the smallest prime divisor of $|G|$. If $\exists\ H \leq G$ with $|G/H| = p$ then $H \trianglelefteq G$.*

Proof. Let N be the normal subgroup contained in H. Note $|G/N| = pk$ and $pk|p!$ which means that $k|(p-1)!$ therefore all prime divisors of k are $< p$. But $k||G|$ so it follows that k has no prime divisors so it is 1 so $|G/N| = p$. □

Def. *N in the n! lemma is the **core** of H. IE if $N = \ker(\varphi)$ where φ is the morphism induced by G on G/H.*

Corrollary. *G finite. If $H \leq G$ and $|G/H| = 2$ then $H \trianglelefteq G$.*

5.2 p-groups

Def. *Let p prime. A **p-group** is a group of order p^k, where $k \geq 0$. (Note that infinite p groups make sense by we won't consider them).*

Corrollary (Fixed Point Lemma for p-groups)**.** *Let G be a p-group, Ω a finite set. G acts on Ω. Then $|\Omega^G| \equiv |\Omega| \pmod p$.*

Proof. A proper subgroup H has index $|G/H| = p^i$. We apply FPL and we are done. □

Corrollary. *Let G be a non trivial p group. Then $Z(G) \neq \{1\}$.*

Proof. Let G act on itself by conjugation. Then $G^G = Z(G)$. By fixed point lemma, we have that $|Z(G)| \equiv |G| \not\equiv 1 \pmod p$. □

Corrollary. *Every p-group is nilpotent.*

Proof. $G/Z(G)$ is a p-group. $|G/Z(G)| < |G|$. By induction $G/Z(G)$ is nilpotent so G is nilpotent (previous prop). $\square$

Lemma. *Let G be a finite abelian group and p a prime divisor of $|G|$. Then G contains an element of order p.*

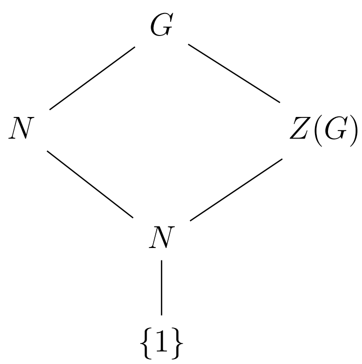
Proof. HW 1, Ex 17. $\square$

Theorem 5.1. *Let G be a nontrivial p-group.*

1. *(big center) If $N \trianglelefteq G$, $N \neq \{1\}$ then $Z(G) \cap N \neq \{1\}$.*
2. *(subgroups of all possible orders) If $N \trianglelefteq G$ and $d||N|$. Then N has a subgroup of order d that is normal in G.*
3. *(normalizers grow) If $H < G \implies H < N_G(H) \leq G$.*
4. *(maximal subgroups) If $K < G$ is a maximal subgroup, then $K \lhd G$ and $|G/K| = p$.*

Proof.

1. Apply FPL to action of G on N by conjugation.
2. Write $d = p^\alpha$. Induct on α. If $\alpha = 0$ done. If $\alpha \geq 1$, then $N \neq \{1\}$ so $Z(G) \cap N \neq \{1\}$. $N \cap Z(G)$ is abelian, so it has a subgroup of order N_1 of order p. $N_1 \subseteq Z(G)$ so $N_1 \trianglelefteq G$.



Consider G/N_1 we have $N/N_1 \trianglelefteq G/N_1$ and $p^{\alpha-1}$ divides $|N/N_1|$. By induction hypothesis, N/N_1 has a subgroup of order $p^{\alpha-1}$ that is normal in G/N_1.

By 4th isomorphism theorem, this subgroup has form N_2 where $N_1 \leq N_2 \leq N$ and $N_2 \trianglelefteq G$. $|N_2| = |N_2/N_1| \cdot |N_1| = p^\alpha$.

3. Let $\Omega = G/H$ and let h act on G/H by $h \cdot xH = hxH$. We see that $xH \in \Omega^H \iff hxH = xH$ for all $h \in H \iff x^{-1}hx \in H \iff h \in xHx^{-1}\ \forall h \in H \iff H \subseteq xHx^{-1} \iff x \in N_G(H)$. Therefore $\Omega^H = N_G(H)/H$ so we want $|\Omega^H| > 1$. By FPL, $|\Omega^H| \equiv |\Omega| \equiv 0 \pmod p$ so it is greater than 1.

4. $K \triangleleft N_G(K) \leq G$ but no bigger subgroups, so it is G. G/K is a p-group has no proper subgroups so cyclic of prime order so $|G/K| = p$.

$\square$

5.3 Sylow Theorems

Def. *G finite group, p prime. Write $|G| = p^\alpha m$ with $\alpha \geq 0$ and $p \nmid m$. A* ***p-Sylow subgroup / p-Sylow*** *of G is a subgroup S with $|S| = p^\alpha$. Let $\mathrm{Syl}_p(G)$ be the set of all p-sylow subgroups of G.*

Theorem 5.2 (first Sylow)**.** *G finite, p prime, $\mathrm{Syl}_p(G) \neq \emptyset$.*

Proof. Induction on $|G|$. Alternatively (a) or (b)

(a) If G has a proper subgroup H of index coprime to p. Then $|H| = p^\alpha m'$ with $p \nmid m'$. Then $\mathrm{Syl}_p(H) \neq \emptyset$ and $\mathrm{Syl}_p(H) \subseteq \mathrm{Syl}_p(G)$.

(b) If G has a nontrivial normal p-subgroup N, then apply induction hypothesis to G/N and so there exists a $S/N \in \mathrm{Syl}_p(G/N)$ where $|S/N| = p^{\alpha-\beta}$ so $N \leq S \leq G$ and $|S| = p^\alpha$.

$$\begin{tikzcd}[arrows=dash]
G \arrow[d] & G/N \arrow[d, "p^{\alpha-\beta}m"] \\
N \arrow[d, "p^\beta"] & \{1\} \\
\{1\} &
\end{tikzcd}$$

If (a) doesn't hold then all proper subgroups have index p. By FPL applied to conjugation action of G onto itself, then $|Z(G)| \equiv |G| \pmod p$. $Z(G)$ is abelian so by lemma this has a subgroup of order p which implies (b). $\square$

Corrollary (Cauchy)**.** *G finite $p \mid |G|$ then there is a subgroup of order p.*

Theorem 5.3 (Second Sylow)**.** *Let G be finite and $S \in \mathrm{Syl}_p(G)$ then $\mathrm{Syl}_p(G) = \{xSx^{-1} : x \in G\}$. In fact, letting $P \leq G$ a p subgroup then $P \subseteq xSx^{-1}$ for some $x \in G$.*

Proof. Let $\Omega = G/S$ Let P act on Ω by $g \cdot \overline{x} = \overline{gx}$. By FPL (since P is p-group), $|\Omega^P| \equiv |\Omega| \not\equiv 0 \pmod p$. So $\Omega^p \neq \emptyset$ so there is a fixed point. Let $\overline{x} \in \Omega^p$. This means that $\overline{gx} = \overline{x}$ so in particular $x^{-1}gx \in S$ for all $g \in P$ so $x^{-1}Px \subseteq S$. $\square$

Corrollary. *$S \in \mathrm{Syl}_p(G)$then $S \trianglelefteq G \iff \mathrm{Syl}_p(G) = \{S\}$.*

6 September 17

6.1 Sylow Theorems Continued

$\mathrm{Syl}_P(G) \neq \emptyset$ and $S \in \mathrm{Syl}_p(G)$ implies that $\mathrm{Syl}_p(G) = \{gSg^{-1} : g \in G\}$.

Lemma. *Let $S, T \in \mathrm{Syl}_p(G)$ s.t. S normalizes T. Then $S = T$.*

Proof.

$$\begin{tikzcd}
 & G \arrow[d, no head] & \\
 & N_G(T) \arrow[dl, no head] \arrow[dr, no head] & \\
S & & T
\end{tikzcd}$$

Note that $S, T \in \mathrm{Syl}_p(N_G(T))$ since both are of order $|p|^\alpha$. $T \trianglelefteq \mathrm{Syl}_p(N_G(T))$ so $S = T$ as they are conjugate. $\square$

Theorem 6.1 (Third Sylow Theorem)**.** *Let $S \in \mathrm{Syl}_p(G)$.*

1. *$n_p(G) = |G/N_G(S)|$*
2. *$n_p(G) \mid m$ where $|G| = p^\alpha m$ with $p \nmid m$.*
3. *$n_p(G) \equiv 1 \pmod p$.*

Proof.

1. $\Omega = \{X \subseteq G, |X| = p^\alpha\}$. G acts on Ω by conjugation. $S\ in \Omega$ since it is of order p^α. $O_G(S) = \mathrm{Syl}_p(G)$ by the second sylow theorem. $S_G(S) = \{g \in G : gSg^{-1} = S\} = N_G(S)$. We have by orbit-stabilizer reciprocity we have the desired.

2. This follows as $|G:S| = |G|/|S| = m$ and $|G:N_G(S)| = n_p(G)$ with $|G:N_G(s)| \mid m$.

$$\begin{tikzcd}[row sep=large] G \arrow[d, no head] \\ N_G(S) \arrow[d, no head] \\ S \arrow[d, no head, "p^\alpha"] \\ \{1\} \end{tikzcd}$$

3. Let S act on $\mathrm{Syl}_p(G)$ by conjugation (it does by second sylow). $|\Omega| = n_p(G)$ and $\Omega^S = \{T \in \mathrm{Syl}_p(G) : T \text{ normalizes } S\} = \{S\}$ by our lemma. Therefore, we apply the fixed point lemma and are done.

$\square$

Prop 6.1 (Frattini's argument)**.** *G arbitrary group, $N \trianglelefteq G$ and finite. Let $S \in \mathrm{Syl}_p(N)$ (for some prime p) and $H = N_G(S)$. Then $G = NH$.*

Proof. Let $g \in G$. We want that $g = nh$ for some $n \in N, h \in H$. Find $n \in N$ s.t. $n^{-1}g \in N_G(S)$ which occurs iff $gSg^{-1} = nSn^{-1}$. Note that $S \leq N$ and $gSg^{-1} \leq gNg^{-1} = N$ therefore gSg^{-1} is a p-sylow in N and there exists an n s.t. nSn^{-1} by second sylow. $\square$

6.2 Direct Groups

Def. *Given groups A and B the direct product is $A \times B$ with product $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2)$ with identity $(1_A, 1_B)$.*

1. *If $A_1 \leq A, B_1 \leq B$ then $A_1 \times B_1 \leq A \times B$.*
2. *$A_1 \times B_1 \trianglelefteq A \times B \iff A_1 \trianglelefteq A, B_1 \trianglelefteq B$.*
3. *A subgroup of $A \times B$ needs not to be of the above for.*

Prop 6.2. *Let $H, K \leq G$ be subgroups. If*

1. *$G = HK$.*
2. *$H, K \trianglelefteq G$.*

3. $H \cap K = \{1\}$.

Then $G \cong H \times K$.

Remark. *The above is iff as we just take* $H = \{(a, 1_B)\}, K = \{(1_A, b)\}$.

Remark. *Let* $H, K \leq G$.

1. $H, K \trianglelefteq G \implies HK \trianglelefteq G$. *If one is normal then it is a subgroup.*

2. *If* $H, K \trianglelefteq G$ *and* $H \cap K = \{1\}$ *then* $hk = kh\ \forall h \in H, k \in K$.

3. *If* H, K *finite then* $|HK| = |H||K|/|H \cap K|$. *Why since no second isomorphism law can be applied?*

4. *If* $\gcd(|H|, |K|) = 1$ *then* $H \cap K = \{1\}$ *by Lagrange.*

6.3 Nilpotent Groups again

Theorem 6.2. *Let* G *be a finite group. The following are equivalent.*

1. G *nilpotent.*

2. *Normalizers grow.*

3. *All Sylow subgroups are normal.*

4. G *is direct product of* p*-groups.*

Proof. For 1 implies 2, note that $G = N_0 \trianglerighteq N - 1 \cdots \trianglerighteq N_k = \{1\}$ be a central series. $N_i \trianglelefteq G$ and $N_{i-1}/N_i \subseteq Z(G/N_i)$. Let $H < G$, $\exists i$ s.t. $N \supseteq N_i$ and $H \not\supseteq N_{i-1}$. We want that $N_G(H) \supseteq N_{i-1}$. Equivalently $[G, N_{i-1}] \subseteq N_i$. This implies that $[H, N_{i-1}] \subseteq [G, N_{i-1}] \subseteq N_i \subseteq H$ which implies that $N_{i-1} \subseteq N_G(H)$.

For 2 implies 3. Let $S \in \mathrm{Syl}_p(G)$. We use HW3 exercise 8 which shows that $N_G(N_G(S)) = N_G(S)$. If $N_G(S) < G$ this implies that $N_G(S) < N_G(N_S(S))$

For 3 implies 4, induction on $|G|$ to show that G is the internal direct product of its nontrivial sylows. $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Let S_i be the unique p-sylow for each i. Let $H = S_1 \dots S_{r-1}$, $K = S_r$. $S_i \trianglelefteq G \implies H \trianglelefteq G, K \trianglelefteq G$. $p_i^{\alpha_i} = |S_i| \mid |H|$ for all $i = 1, \dots, r-1$. Then $|H| \mid p_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}}$ so $|H| = p_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}}$, $|K| = p_r^{\alpha_r}$ by using the property 3 in the above remark. Therefore, $|H \cap K| = \{1\}$, and $|HK| = p_1^{\alpha_1} \dots p_r^{\alpha_r} = |G|$ and G is our direct product of p-groups as we assume H is by induction. Note that H can use this induction (all Sylow subgroups are normal) since all sylows of p are unique (and are unique in G as well).

For 4 implies 1, we show that direct products of p-groups are nilpotent (p-groups are nilpotent). This is HW4 Ex 1. $\square$

Corrollary (Lagrange converse)**.** *Let G be finite nilpotent. For each divisor $d \mid |G|$, there is a normal $N \trianglelefteq G$ with $|N| = d$.*

Proof. We've proven this for our p-groups. $\square$

Theorem 6.3. *Let G be finite. Then G nilpotent $\iff$ all maximal subgroups are normal.*

Proof. Refer to notes. $\square$

7 September 19

7.1 Semidirect Product

We won't cover this, so we cover this ourselves.

Def. *Let G, A be groups. Suppose G acts on A with $G \times A \to A$. We say that the action is* ***by automorphisms*** *if $g \cdot (ab) = (g \cdot a)(g \cdot b)$ for all $g \in G, a, b \in A$.*

Remark.

(a) $g \cdot 1_A = 1_A$.

(b) Let $\varphi : G \to S(A)$ be the associated morphism of groups. Then $\mathrm{Aut}(A) = \{\sigma \in S(A) : \sigma$ *is an isomorphism*$\}$. $\mathrm{Aut}(A) \leq S(A)$ *and the action is by automorphism iff* $\operatorname{im}\varphi \subseteq \mathrm{Aut}(A)$. $\varphi_g(ab) = g \cdot ab = (g \cdot a)(g \cdot b) = \varphi_g(a)\varphi_g(b)$, *so this is equivalent to saying φ_g is an automorphism of A.*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[dr, dotted] & S(A) \\ & \mathrm{Aut}(A) \arrow[u, hook] \end{tikzcd}$$

Ex. *$G \times G \to G, g \cdot h = ghg^{-1}$ is by automorphisms. $G \times G \to G, g \cdot g = gh$ is not by automorphisms.*

Def. *Suppose G acts on A by automorphisms. Then we have the* ***semi-direct product*** *$A \rtimes G$ is defined s.t. the underlying set $A \times G$ and $(a, g)(b, h) = (a(g \cdot b), gh)$. The unit is $(1_A, 1_G)$.*

Prop 7.1. *$A \rtimes G$ is a group. Proof is optional.*

Remark. *$A \rtimes G$ depends on the action. If the action changes then the semidirect product is different. We also want to show that $G \cong A \rtimes B$ for some A, B and some action.*

7.2 Hall Subgroups

Def. *Let π be a set of primes and n a positive integer. The* ***π-part*** *of n is the highest divisor of n involving primes from π* ***only***. *The* ***π'-part*** *of n is the highest divisor of n not involving any of the primes in π.*

Ex. $n = 60 = 2^3 \cdot 3 \cdot 5$. $\pi = \{2, 3\}$ *then the π-part is* 12 *and the π'-part is* 5.

Def. *Let G be a group and $H \leq G$. Let π be a set of primes. We say that H is a* ***π-hall*** *subgroup of G if $|H|$ is a π-part of $|G|$.*

Remark.

1. *If $\pi = \{p\}$, then π-halls are p-sylow.*
2. *$H \leq G$ is a π-hall for some π iff* $\gcd(|H|, |G/H|) = 1$.

Our goal is that G finite solvable implies that π-Hall exist for all π, an analogue to first Sylow Theorem.

Lemma. *Let G be a finite solvable group and M is minimal normal subgroup (such a subgroup always exists). Then M is elementary abelian (homework). In particular M is a p-group for some prime p.*

Proof. Homework 2 Ex 4. □

Lemma. *G finite solvable and $N \lhd G$ then $\exists$ a prime p and a p-subgroup P s.t. $N < NP \trianglelefteq G$.*

Proof. $N < G \implies G/N \neq \{1\}$ so there is a minimal normal subgroup of G/N. Since G is solvable, then G/N is solvable, which implies this subgroup is a p-subgroup for some p. It is of the form M/N with $N < M <\trianglelefteq G$. Let P be a p-Sylow of M (P is a p-subgroup of G). Let P be a p-Sylow of M, then we see that $|M/N|$ is a power of p and $|M/P|$ is prime to p since P is a p-Sylow. Then that implies that $|M/NP| = 1$ as this divides for $|M/P|$ and $|M/N|$ so $NP = M$. □

Theorem 7.1 (Schur-Zassenhaus). *G finite and N a normal Hall subgroup of G. Then N has a complement in G: $\exists H \leq G$ s.t. $G = NH$ and $N \cap H = \{1\}$.*

Proof. We assume G is solvable since this is too big for our class.

Claim: It suffices to find $H \leq G$ with $|H| = |G/N|$. For then: $|N \cap H$ divides both $|N|$ and $|G/N|$ which implies that $N \cap H = \{1\}$ and then $|NH/N| = |H/H \cap N| = |H| = |G/N| \implies |NH| = |G|$.

We induct on $|G|$. If $|G| = 1$ then this is true. if $N = G$ this is true. Assume $N < G$. By Lemma 2, $\exists p$ subgroup P s.t. $N < NP \trianglelefteq G$.

$$\begin{tikzcd}[column sep=small]
 & G \arrow[d, dash] & \\
 & NP \arrow[dl, dash] \arrow[dr, dash] & \\
N \arrow[dr, dash] & & P \arrow[dl, dash] \\
 & N \cap P \arrow[d, dash] & \\
 & \{1\} &
\end{tikzcd}$$

1. $|P|$ is a power of p.
2. $|P/N \cap P|$ is a power of p since it divides $|P|$.
3. $|NP/N|$ is a power of p by NH diamond.
4. $|G/N|$ is divisible by p.
5. $|N|$ prime to p (N is Hall).
6. $|N/N \cap P|$ is prime to p.
7. $|NP/P|$ is prime to p.
8. $P \in \mathrm{Syl}_p(NP)$.

Is P a complement of N? We note that $|N \cap P$ divides both $|N|$ and $|P|$ so $N \cap P$ is $\{1\}$, but this is still not enough to get our value. So we enlarge P and let $K = N_G(P)$ and we have that $G = NPK = NK$ by Frattini.

IS K a complement of N? Slice off $N \cap K$ from K using induction hypothesis.

- Can we? $N \cap K \trianglelefteq K$ because $N \trianglelefteq G$.
- If $N \cap K$ a Hall subgroup of K? Well we see that $|K/N \cap K| = |G/N|$ is prime to $|N|$, so it is prime to $|N \cap K$ so yes.
- K is solvable since G is.

We need $|K| < |G|$.

- If $|K| < |G|$ by induction $\exists$ complement H of $N \cap K$ with K. In particular $|H| = |K/N \cap K| = |G/N|$ so H is a complement of H in G by our claim.
- If $|K| = |G|$ then P is normal in G. Consider G/P. We claim that NP/P is a normal Hall subgroup of G/P. $|NP/P| = |N/N \cap P| = |N|$ (using NP diamond). $|\frac{G/P}{NP/P}| = |G|/|NP| = |G/N|/|P|$. Since $|N$ is prime to $|G|/|N|$, NP/P is Hall inside G/P. By induction we have complement H/P of NP/P in G/P and see that $|H| = |G/N|$ so H is a complement of N in G.

$\square$

Theorem 7.2 (Hall)**.** *G finite solvable. For any set of primes π. There exists a π-Hall subgroup of G.*

Proof. Induction on $|G|$. If $G = \{1\}$ let M be a minimal normal subgroup. If G is solvable then M is a p-subgroup. By induction hypothesis, there exists a π-hall subgroup of G/M. It is of the form K/M for some $M \leq K \leq G$.

$$\begin{tikzcd}
G \arrow[d, dash] & G/M \arrow[d, dash] \\
K \arrow[d, dash] & K/M \arrow[d, dash] \\
M & \{1\}
\end{tikzcd}$$

$|K| = |K/M||M|$ involved only primes in $\pi \cup \{p\}$. $|G/K|$ involved only primes in π'.

- If $p \in \pi$ then K is a π-Hall.

- If $p \notin \pi$ then we want to slice M from K. Note that M is a Hall subgroup as $|K/M|$ does not involve p and $|M|$ is a power of p and $\gcd(|K/M|, |M|) = 1$. Also, $M \trianglelefteq K$ since $M \trianglelefteq G$. By S-Z, exists a complement H of M in K. $|H| = |K/M|$ induces only primes in π. Furthermore $|G/H| = |G/K| \cdot |M|$ involves only primes in $\pi' \cup \{p\} = \pi'$ so H is a π-Hall.

$\square$

7.3 Looking Forward

Theorem 7.3. *Let G be a finite solvable group. Then*

1. *Any two π-Halls are conjugate.*
2. *If $K \leq G$ with $|K|$ involves primes in π only, this implies there exists a π-Hall H that contains K.*

Theorem 7.4. *If π-Halls exist for all π then G is solvable.*

Theorem 7.5 (Burnside)**.** *If $|G| = p^a q^b$ then G is solvable.*

Theorem 7.6 (Feit Thompson)**.** *All groups of odd order are solvable.*

8 September 24

8.1 Simple Groups

Remark. *Recall: let G act on Ω and $\varphi : G \to S(\Omega)$. The action is **faithful** if $\varphi : G \hookrightarrow S(\Omega)$ or $\ker(\varphi) = \{1\}$ or $\bigcap_{\alpha \in \Omega} S_G(\alpha) = \{1\}$ or no nontrivial g fix all elements of Ω. The action is **transitive** if for all α, β then there is a g s.t. $g \cdot \alpha = \beta$. In this case all stabilizers are conjugate since all elements are in one orbit.*

Def. *Consider $\Omega^2 \setminus \triangle = \{(\alpha, \alpha') \in \Omega^2 : \alpha \neq \alpha'\}$. Suppose $g\alpha = g\alpha' \implies \alpha = \alpha'$. G acts on $\Omega^2 \setminus \triangle$ via $g \cdot (\alpha, \alpha') = (g \cdot \alpha, g \cdot \alpha')$. The action of G on Ω is 2-**transitive** if its action on $\Omega^2 \setminus \triangle$ is transitive. This means that given $\alpha \neq \alpha'$ and $\beta \neq \beta'$ in Ω, $\exists g \in G$ s.t. $g \cdot \alpha = \beta$ and $g \cdot \alpha' = \beta'$.*

Ex. *The action of S_n on $[n]$ is 2-transitive for all $n \geq 1$. If $n = 1$ the condition is vacuous. If $n \geq 2$ given $a \neq a'$ and $b \neq b'$ in $[n]$¿ Pick any bijection $\tau : [n] \setminus \{a, a'\} \to [n] \setminus \{b, b'\}$. Define $\sigma : [n] \to [n]$ by $\sigma(a) = b, \sigma(a') = b'$, $\sigma(i) = Z(i) \forall i \in [n] \setminus \{a, a'\}$. Then $\sigma \in S_n$ and $\sigma \cdot a = b, \sigma \cdot a' = b'$.*

Prop 8.1. *Suppose G acts on Ω 2-transitively. Then*

(a) It is transitive.

(b) If $|\Omega| \geq 2$ all stabilizers are maximal subgroups.

Proof. (a) If $|\Omega| = 1$ nothing to do . If $|\Omega| \geq 2$ Take $\alpha, \beta \in \Omega$. Pick any $\alpha' \in \Omega \setminus \{\alpha\}, \beta'$ similarly. By two transitivity there exists a g s.t. $(g\alpha, g\alpha) = (\beta, \beta')$.

(b) Let $\alpha \in \Omega$ and $H = S_G(\alpha)$. If $H = G$, then $\Omega = \{1\}$. But this isn't true since $|\Omega| \geq 2$ so $H < G$. Suppose $\exists K$ w.t. $H < K < G$. Then there exists a $g \in G \backslash$K and a $k \in K \setminus H$. Since $k, g \notin H \implies x \neq k \cdot \alpha$, $\alpha = g\alpha$. Which implies that $\exists f \in G$ s.t. $f\alpha = \alpha, fk\alpha = g\alpha$ which implies that $f \in S_G(\alpha) = H$ and $k^{-1}g^{-1}g \in S_G(\alpha) = H$. This imlpies that $g \in fkH \in HKH = K$ which implies that H maximal as this is a contradiction.

□

Def. *A group is* ***perfect*** *if $G' = [G, G] = G$.*

Remark.

1. *If G is solvable and nontrivial then G is not perfect.*
2. *G simple and nonabelian implies that G is perfect.*
3. *Not every perfect group is simple. Let S be a simple nonabelian group and take $G = S \times S$. G is non simple but $G' = S' \times S' = S \times S = G$ so G is perfect.*

Theorem 8.1 (Iwasawa's Lemma)**.** *Let G be a nontrivial perfect group. Suppose G acts on Ω s.t.*

1. *The action is faithful and 2-transitive.*
2. *There exists a stabilizer H that contains a subgroup A s.t.*

   (i) $A \trianglelefteq H$.
   (ii) A is abelian.
   (iii) The set $\bigcup_{g \in G} gAg^{-1}$ generates G.

   Then G is simple.

Remark. *Under a all stabilizers are conjugate. Hence if b holds for one stabilizer it holds for all stabilizers.*

Proof. G nontrivial and faithful implies $|\Omega| \geq 2$ because $G \hookrightarrow S(\Omega)$. Now 2 transitive implies that stabilizers are maximal. Let $\{1\} \leq N \trianglelefteq G$. If N is contained in all stabilizers then $N = \{1\}$ by faithful. Otherwise, $\exists$ stabilizer H s.t. $N \not\subseteq H$ then that implies that $H < NH \leq G$ which implies that $NH = G$ by maximality. We can assume H satisfies b. let $g \in G \implies g = nh, n \in N, h \in H$ which implies that $gAg^{-1} = nhAh^{-1}n^{-1} = nAn^{-1}$ since $A \trianglelefteq H$ and is a subset of $NAN = NNA$ as N is normal so $G = NA$. Note that $G/N = NA/N \cong A/N \cap A$ is abelian so $[G,G] \subseteq N$. $\square$

8.2 The alternating groups

Remark. *Some facts about A_n from HW 5.*

1. *The $(2,2)$ cycles form a conjugacy class in A_n for every $n \geq 4$.*
2. *The 3 cycles generate A_n for $n \geq 4$.*
3. *The $(2,2)$ cycles generate A_n for $n \geq 5$.*
4. *A_n is perfect for $n \geq 5$ since $[(a,b,c),(a,b,d)] = (ab)(cd)$.*

Corrollary. *A_5 is simple.*

Proof. A_5 acts on $[5]$ faithfully since A_5 is a subgroup of S_5. Is it 2-transitive, we can check. Let $H = S_{A_5}(5) \implies H \cong A_4$. Let $A = \{1, (12)(34), (13)(24), (14)(23)\} \cong V_4$. Then $A \trianglelefteq H$ and $A \cong V_4$ and is abelian. The conjugates of A in A_5 consist of all $(2,2)$ cycles. Use use Iwasawa's to prove that this is simple. $\square$

Remark. *Can we do the same proof for $n \geq 6$? Well A_n is perfect, it is faithful and 2-transitive. The stabilizers of a point $\cong A_{n-1}$ simple so there are no normal subgroups so we can't use this. We can prove separately using induction.*

9 September 26

9.1 The Projective Special Linear Groups

Def. *Let $\mathbb{F}$ be a field. Then $PGL(n,\mathbb{F}) = GL(n,\mathbb{F})/Z(GL(n,F))$ and $PSL(n,\mathbb{F}) = SL(n,\mathbb{F})/Z(SL(n,\mathbb{F}))$. Note that $Z(GL(n,\mathbb{F})) = \{aI_n : a \in \mathbb{F}^\times\}$ and $Z(SL(n,\mathbb{F})) = \{aI_n : a \in \mu_n(\mathbb{F})\}$ through computation. We will write $GL(n,\mathbb{F}_q) = GL(n,q)$ and similarly for all others.*

$$
\begin{tikzcd}
SL(n,\mathbb{F}) \arrow[r, hook] \arrow[d, two heads] & GL(n,\mathbb{F}) \arrow[d, two heads] \\
PSL(n,\mathbb{F}) \arrow[r, hook] & PGL(n,F)
\end{tikzcd}
$$

Remark.

1. $|GL(n,q)| = (q^n - 1)\dots(q^N - q^{n-1})$.
2. $\mathbb{F}_2^\times = \{1\}$ *then all four groups are the same.*
3. $PGL(1,\mathbb{F}) = \{1\}$.
4. $PSL(2,2) \cong S_3, PSL(2,3) \cong A_4$. *The goal is the for other* $PSL(2,q)$ *is simple for* $n > 2$ *or* $n = 2, q > 3$.

Lemma. $\mathbb{F}$ *any field implies that* $SL(2,\mathbb{F})$ *is generated by* $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ *and* $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$.

Proof. Take $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{F})$.

- If $b \neq 0$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (d-1)/b & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a-1)/b & 0 \end{pmatrix}$$

- If $c \neq 0$ then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & (a-1)/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & (d-1)/c \\ 0 & 1 \end{pmatrix}$$

- If $b = c = 0$ then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ d-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix}$$

□

Remark. *Notation is* $U = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\}, B = \{\begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix}, a \in \mathbb{F}^x, b \in F\}$.

Lemma.

(a) $U \trianglelefteq B \trianglelefteq SL(2, \mathbb{F})$.

(b) $B \cong U \rtimes \mathbb{F}^\times$.

(c) U *is abelian.*

(d) U *and its conjugates generate* $SL(2, \mathbb{F})$.

Proof. $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b + b' \\ 0 & 1 \end{pmatrix}$ so $U \cong (\mathbb{F}, +)$. Similarly,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix}$$

□

Lemma. *If* $|\mathbb{F}| \geq 4$ *(possibly infinity) then* $SL(2, \mathbb{F})$ *is perfect.*

Proof. Suffices to check that all elements $u \in U$ are commutators. Note that

$$\left[\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (a^2 - 1)b \\ 0 & 1 \end{pmatrix}$$

It suffices that $\forall c \in \mathbb{F}$ there exists $a \in \mathbb{F}^\times, b \in F$ s.t. $c = (a^2 - 1)b$. Similarly, it suffices to find $a \in \mathbb{F}^\times$ s.t. $a^2 - 1 \neq 0$ or $a \in F$ s.t. $a^3 - a \neq 0$. This is true because $|\mathbb{F}| \geq 4$. □

Remark. *Recall the projective line* $= \mathbb{P}^1(\mathbb{F})$ *being the set of lines through* 0 *in* $\mathbb{F}^2$. $GL(2, \mathbb{F})$ *acts on* $\mathbb{F}^2$ *by* $A \cdot v = Av$.

Lemma. *The action of* $SL(2, \mathbb{F})$ *on* $\mathbb{P}^1(\mathbb{F})$*:*

(a) *Is* 2*-transitive.*

(b) *The stabilizer of the* x*-axis is* B.

(c) *The kernel of the action is* $Z(SL(2, \mathbb{F}))$.

Proof. Let (ℓ_1, ℓ_2) and (r_1, r_2) be pairs of lines with $\ell_1 \neq \ell_2, r_1 \neq r_2$. We need that $A \in SL(2, \mathbb{F})$ s.t. $A\ell_1 = r_1, A\ell_2, r_2$. Choose $v_1 \in \ell_1, v_2 \in \ell_2, w_1 \in r_1, w_2 \in r_2$ nonzero vectors. Then $\{v_1, v_2\}$ and $\{w_1, w_2\}$ are bases of $\mathbb{F}^2$. This implies that there exists $A \in GL(2, \mathbb{F})$ s.t. $Av_i = w_i$ for $i = 1, 2$. □

Theorem 9.1. *IF* $|\mathbb{F}| \geq 4$ *then* $PSL(2, \mathbb{F})$ *is simple.*

Proof. The definition of $PSL(2, \mathbb{F})$; it is the mod operation of $SL/Z(SL)$. We examine Iwasawa.

- It is perfect as shown in a previous lemma.
- 2 transitive, faithful action.
- $\overline{B}$ is stabilizer, $\overline{U}$ is an abelian normal subgroup. $\overline{U}$ and its conjugates generate.

$\square$

Remark. *GL acts on $\mathbb{P}^1(\mathbb{F})$. This is not faithful and group is not perfect since $[GL, GL] \leq SL < GL$. SL is not faithful but is perfect. PGL is faithful but not perfect. PSL is the one which is faithful and perfect. A_n and S_n. S_n is faithful and not perfect.*

Theorem 9.2. *If $n \geq 3$, $PSL(n, \mathbb{F})$ is simple for any $\mathbb{F}$.*

Proof. $PSL(n, \mathbb{F})$ acts on $\mathbb{P}^{n-1}(\mathbb{F})$ (set of line in n-dimensional space). The action is two transitive (pick bases again) and the kernel is $Z(SL(n, \mathbb{F}))$. The stabilizer of the line spanned by $(1, 0, \dots, 0) \in \mathbb{F}^n$ is

$$\left\{ \begin{pmatrix} a & v \\ 0 & A \end{pmatrix} : a \in \mathbb{F}^\times, A \in GL(n-1, \mathbb{F}), v \in \mathbb{F}^{n-1}, a \det(A) = 1 \right\}$$

B contains an abelian normal subgroup

$$U = \left\{ \begin{pmatrix} 1 & v \\ 0 & I_{n-1} \end{pmatrix} \right\}$$

U and its conjugates generate $SL(n, \mathbb{F})$ because any matrix in $SL(n, \mathbb{F})$ is a product of elementary matrices. $E_{i_j}(\lambda) = I_n + \lambda e_{ij}$ with $i \neq j$, $\lambda \in F$. For $n \geq 3$ $SL(n, \mathbb{F})$ is perfect

$$\left[\begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & \lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_{13}(\lambda)$$

$\square$

Remark. $|PSL(n, q)| = |GL(n, q)|/(\gcd(n, q-1) \cdot (q-1))$. *With that we can compute the orders of the first groups of that family*

n/q	*2*	*3*	*4*	*5*	*7*
2	*6*	*12*	*60*	*60*	*168*
3	*168*	*5616*	*20160*	*37200*	
4	*20160*				

And we see that

1. $PSL(2,2) \equiv S_3, PSL(2,3) \equiv A_4$.
2. *There exists a unique simple group of order* 60 $PSL(2,4) \cong PSL(2,5) \cong A_5$.
3. *There exists a unique simple group of order 168 so* $PSL(3,2) \cong PSL(2,7)$.
4. $PSL(4,2) \cong A_8$ *but* $PSL(3,4) \neq A_4$.

10 Oct 1

10.1 Classification of Simple Groups

In notes.

10.2 Projective Geometries

Def. *An **incidence geometry** of rank* 2 *(**plane**) is a* $g = (g_0, g_1, R)$ *where* g_0 *and* g_1 *are sets and* R *is a relation between the two sets. Also known as a **bipartite graph**. The elements of* g_0 *are called **points**, the elements of* g_1 *are **lines**. We say* p ***lives** in* ℓ *or* ℓ ***goes through*** p *or that* p *and* ℓ *are **incident** if* $p \sim \ell$. *Note that in* $\mathbb{R}^2$ g_0 *is* $\mathbb{R}^2$ *and* g_1 *are lines in* $\mathbb{R}^2$.

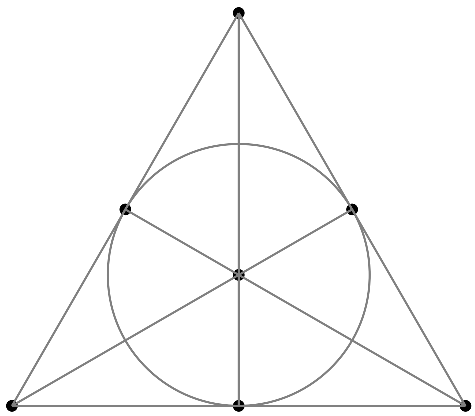
Def. *A plane is **projective** if*

- *Given* 2 *distinct points there is a unique line going through them. IE exists unique* ℓ *s.t.* $p \sim \ell, q \sim \ell$.
- *Given* 2 *distinct lines, there exists a unique points that lies in both.*
- *There are at least* 3 *noncollinear points.*

Ex.

1. *The smallest projective plane is* 3 *points with lines pairwise.*

2. *With 4 points none collinear. If we connect them pairwise, we have a problem since for line bc there is no intersection with ad So, we need to create new points $a' \in \overline{bc}$. Also, we need to have a line connecting a', b', c' and this is enough. Thi is the Fano plane $\mathcal{F}$.*



3. *Let $\mathbb{F}$ be a field. let $PG(2, \mathbb{F})$ be the plane with points being the 1-dimension subspaces of $\mathbb{F}^3$ and the lines are 2-dim subspaces of $\mathbb{F}^3$. We can check the axioms.*

Prop 10.1. *$PG(2, \mathbb{F}_2) \cong \mathcal{F}$.*

Proof. $\mathbb{F}_2^3 = \{(000), \ldots, (111)\}$. Points are lines through the origin and these are the multiples of nonzero vector (7 possibilities) and each point in the $\mathbb{F}_2^3$ determines a unique point in our plane. Lines are the 3 types of coordinate planes which are $x = 0, x + y = 0, x + y + z = 0$. Note that $x + y + z = 0$ consists of origin and 3 points (110) permuted. We have 7 planes. IN particular the points (from top left to bottom right) is $(001), (101), (011), (111), (100), (110), (010)$. $\square$

Remark. *Projective geometries except for rank 2 are of the form $PG(n, \mathbb{F})$ where $\mathbb{F}$ is a division ring.*

Def. *A **symmetry** of a plane g is a pair $\sigma = (\sigma_0, \sigma_1)$ where $\sigma_i : g_i \to g_i$ are bijection s s.t. p incident to ℓ iff $\sigma_0(p)$ incident to $\sigma_1(\ell)$. Let $\mathrm{Aut}(g)$ be the set of all symmetries of g. It is a group under composition.*

Lemma. *$|\mathrm{Aut}(\mathcal{F})| \leq 168$.*

Proof. Choose 3 noncollinear points in $\mathcal{F}$ pqr. Consider the function $\mathrm{Aut}(\mathcal{F}) \to \{(x, y, z) \in \mathcal{F}_0^3 : x \neq y, x \neq z, y \neq z\}$ by $\sigma \to (\sigma_0(p), \sigma_p(q), \sigma_0(r))$. We claim this is injective. To see this, $\sigma_0(p')$ must be third point on $\sigma_0(p)\sigma_0(q)$.

We have 7 choices for $\sigma_0(p)$, 6 for $\sigma_0(q)$, and 4 for the $\sigma_0(r)$ since one of the last elements is collinear with the other 2. Therefore, we see that $|\operatorname{Aut}(\mathcal{F})| \leq 168$. $\square$

Prop 10.2. $\operatorname{Aut}(\mathcal{F}) \cong PSL(3,2) = GL(3,2)$.

Remark. *Recall that* $|GL(3,2)| = (2^3-1)(2^3-2)(2^3-2^2) = 168$.

Proof. $GL(3,2)$ acts on $\mathbb{F}_2^3$ linearly. It preserves i-subspaces ($i = 1,2$). So $GL(3,2)$ acts on $PG(2,\mathbb{F}_2)$ by symmetries which implies that $GL(3,2) \to \operatorname{Aut}(PG(2,\mathbb{F}_2))$. Over $\mathbb{F}_2$ this action is faithful so this is injective. $|GP| = |GL(3,2)| \leq |\operatorname{Aut}(PG(2,\mathbb{F}_2))| = |\operatorname{Aut}(\mathcal{F})| \leq 168$. $\square$

Remark. *One can define projective geometries of higher rank.* $PG(n,\mathbb{F})$ *is a projective geometry of rank* n *for which points are the* 1*-dim subspaces of* $\mathbb{F}^{n+1}$*, lines are* 2*-dim subspaces of* $\mathbb{F}^{n+1}$*, etc...*

Theorem 10.1 (Fundamental Theorem of Projective Geometry)**.** $\operatorname{Aut}(PG(n,\mathbb{F})) \cong PGL(n+1,\mathbb{F}) \rtimes \operatorname{Aut}(\mathbb{F})$.

11 Oct 3

11.1 Monoids

Def. *A* ***monoid*** M *is a set with binary operation satisfying associativity and has identity. Note that this is a group without inverse operation.*

Ex. $\mathbb{N}$ *is a monoid under* $+$.

Def. *Let* M *be a monoid and* $\sim$ *is an equivalence relation on* M*. We say* $\sim$ *is (left, right, two sided)-compatible if* $a \sim b$ *then* $xa \sim xb$*,or for right* $ax \sim bx$*, or for center* $a \sim b, x \sim y \implies ax \sim by$.

Remark. 2 *sided compatible iff both left and right compatible.*

Def. *Let* $\widetilde{M}$ *be the set of equivalence classes defined by* $\overline{a} \cdot \overline{b} = \overline{ab}$.

Prop 11.1. *The operation is well defined iff* $\sim$ *is* 2*-sided compatible. In this case,* $\widetilde{M}$ *is a monoid. The unit is* $\overline{1}$.

Def. *Let* $\pi : M \to \widetilde{M}$, $\pi(a) = \overline{a}$. π *is a morphism of monoids.*

Prop 11.2 (Universal Property of Quotient For Monoids)**.** *Let* $\varphi : M \to N$ *be a morphism of monoids s.t. if* $a \sim b$ *the* $\varphi(a) = \varphi(b)$*. Then* $\exists!$ *morphism of monoids* $\widehat{\varphi} : \widetilde{M} \to N$ *that commutes as shown below.*

$$\begin{tikzcd} M \arrow[r, two heads, "\pi"] \arrow[d, "\varphi"'] & \widetilde{M} \arrow[dl, dotted, "\widehat{\varphi}"] \\ N & \end{tikzcd}$$

Proof. Define $\widehat{\varphi}(\overline{a}) = \varphi(a)$ $\square$

Prop 11.3. *Let G be a group and $\sim$ an equiv relation. Then*

(i) $\sim$ is left compatible iff there is a subgroup $H \leq G$ s.t. $a \sim b \iff a^{-1}b \in H$.

(ii) Right compatible is $ab^{-1} \in H$.

(iii) Two sided compatible is a normal subgroup s.t. either hold.

11.2 Free Monoids

Def. *Let S be a set and let $S^* = \bigcup_{m \geq 0} S^m$ which is the set of all finite sequence of S. A* ***concatenation*** *is $(s_1, \dots, s_i) \cdot (t_1, \dots, t_j) = (s_1, \dots, s_i, t_1, \dots, t_g)$.*

Lemma. *S^* is a monoid under concatenations. The unit is $()$. We define the elements of sS as letters, S is alphabet and S^* is words. Define $i : S \to S^*$ by $s \to (s)$. We say S^* is the* ***free monoid*** *on S.*

Prop 11.4 (Universal Prop of the free monoid)**.** *Let M be a monoid and a map $f : S \to M$. Then $\exists!$ morphism of monoids $f^* : S^* \to M$ s.t.*

$$\begin{tikzcd} S \arrow[r, hook, "i"] \arrow[dr, "f"'] & S^* \arrow[d, dotted, "f^*"] \\ & M \end{tikzcd}$$

Proof. Define $f^*(s_1, \dots, s_n) = f(s_1) \dots f(s_n)$. $\square$

11.3 Free Groups

Remark. *S^* is clearly not a group. Let $\overline{S} = \{\overline{s} : s \in S\}$ be a new copy of S. Let $T = S \cup \overline{S}$ and define operation Let $t^{-1} = \begin{cases} \overline{s} & t = s \in S \\ s & t = \overline{s} \in \overline{S} \end{cases}$. The free monoid T^**

Def. *We say two words $w, w' \in T^*$ has $w \sim w'$ if if we can insert or delete finitely many pairs (t, t^{-1})*

Ex. *$S = \{a, b\}$ and we see that $(ab^{-1}aa^{-1}b) \sim (ab^{-1}b) \sim (a) \sim (bb^{-1}a)$.*

Prop 11.5. *This relation on the monoid T^* is two-sided compatible.*

Def. *$F(S) = \widetilde{T^*} = T^*/\sim$ is a monoid. We can see the operations and unit pretty simply. Let $i : S \to F(S)$ by $i(s) = [s]$.*

Lemma. *$F(S)$ is a group generated by $i(S)$.*

Proof. $[t_1, \ldots, t_n]^{-1} = [t_n^{-1}, \ldots, t_1^{-1}]$. This is trivial by induction. Easy to see that $i(S)$ generates group. $\square$

Prop 11.6 (Universal Prop of Free Group)**.** *Let G be a group and $\varphi : S \to G$ a map. Then $\exists!$ morphism of groups $\widehat{\varphi} : F(S) \to G$ s.t.*

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

Recall that $S \hookrightarrow S^* \twoheadrightarrow F(S)$ is our i.

Proof.

$$\begin{tikzcd} S \arrow[r, hook] \arrow[dr, "\varphi"'] & T \arrow[r, hook] \arrow[d, "\overline{\varphi}"] & T^* \arrow[r, two heads] \arrow[dl, dotted, "\varphi^*"] & F(S) \arrow[dll, dotted, "\widehat{\varphi}"] \\ & G & & \end{tikzcd}$$

Define $\overline{\varphi} : T \to G$ by $\overline{\varphi}(t) = \varphi(t)$ if $t \in S$ otherwise $\varphi(t^{-1})^{-1}$ if $t \in S^{-1}$. BY UP of free monoids, exists unique morphism φ^* on above. We check that $\varphi^*(w) = \varphi^*(w')$. Note that $\varphi^*(w') = \overline{\varphi}(t_1) \ldots \overline{\varphi}(t_n)$. By UP of quotients for monoids, exists a unique morphism of monoids $\widehat{\varphi} : F(S) \to G$ (and since both are groups it is a morphism of groups). This is unique as must show that $\overline{\varphi}$ is unique. $\square$

12 Oct 8

12.1 More on Free Groups

Def. *A pair of consecutive letters in a word $w \in T^*$* ***cancellable*** *if it is of the from tt^{-1}.*

Remark. *Recall that $F(S) = T^*/\sim$ where $w \sim w'$ if one is obtained from the other by a finite sequence of intersections and deletions of cancellable pairs.*

Def. *A word $w \in T^*$ is **reduced** if it contains no cancellable pairs.*

Prop 12.1. *Each equivalence class contains exactly one reduced word. Then $F(S)$ is bijective, with the set of reduced words.*

Corrollary. *$i : S \to F(S), s \to [s]$ is injective.*

Proof. Suppose $[s_1] = [s_2] \implies (s_1) \sim (s_2)$. This means they are reduced and therefore are equal. □

Ex. *$S = \emptyset \implies F(S) = \{1\}$. $S = \{a\} \implies F(s) = \{a^n : n \in \mathbb{Z}\}$. So isomorphism from $\mathbb{Z} \to F(a)$ $n \to a^n$. $S = \{a, b\}$ is more complicated. It ends up forming a fractal tree, with each having 4 branches for a, a^{-1}, b, b^{-1}.*

Proof. Given a class, choose a representative w. If w is reduced, we are done. If not, it contains a cancellable pair. Remove it and get word $w' \sim w$. Eventually must stop and by induction on length, exists reduced word. Suppose $w_1 \sim w_2$. WE can draw a diagram that goes up and down for insertion and deletion. We claim that w_1 to w_2 is a valley. The proof follows since we can't go down since w_1, w_2 are reduced.

To prove that claim, it suffices to show that each peak into a valley. We can invert each peak and then we have 1 less peak. Repeat until it's no peaks. This property is called **confluence**.

To prove confluence, it suffices to prove that special case in which one side of the peak is length 1. In particular, we prove that we can resolve a peak of both sides 1 to a valley of both sides at most 1. We prove this. There are 3 cases: they are disjoint, so they can be reversed, insertion is $i(id)d$, and these can be swapped. □

12.2 Presentations

Def. *Let S be a set. Consider words in T^*. Let N be the smallest normal subgroup of $F(S)$ containing $[w_i][w_i]^{-1}$ for $i \in [n]$. The **group generated by S subject to the relation** $w_i \equiv w_i'$ is $\langle s : w_i \equiv w_i' \rangle = F(S)/N$ (group presentation)*

Ex. *$D_n = \langle \rho, \sigma : \rho^m = 1, \rho\sigma = \sigma\rho^{-1} \rangle$ then $\mathbb{Z}_n = \langle \rho \rangle$.*

Prop 12.2. *Let $\varphi : S \to G$ be a map s.t. $\varphi(w_i) = \varphi(w_i')$ for all $i \in [m]$. then exists a unique group morphism $\widehat{\varphi} : \langle s : w_i \equiv w_i' \rangle \to G$ s.t.*

$$\begin{tikzcd}
S \arrow[r, "i"] \arrow[dr, "\varphi"'] & F(s) \arrow[r, two heads] \arrow[d, dotted, "\widehat{\varphi}"] & \langle s : w_i \equiv w_i' \rangle \arrow[dl, "\widehat{\varphi}"] \\
& G &
\end{tikzcd}$$

12.3 Zorn's Lemma

Def. *A **poset** is partially ordered set. A **chain** in X is a subset C that is totally ordered.*

Remark.

- *A chain may be uncountable.*
- *$\emptyset$ is a chain in any poset X*
- *ϕ has a upper bound iff X is nonempty.*

Def. *Given a subset S of a poset X, an **upper bound** for S is an element $x \leq u$ for all $x \in S$.*

Def. *An element $m \in X$ is maximal if $\nexists x \in X$ s.t. $m < x$. it is maximum if $x \leq m$ for all $x \in X$. Note that maximum implies maximal.*

Lemma (Baby Zorn's Lemma)**.** *Let X be a finite nonempty poset. Then X has a maximal element.*

Proof. Induction. □

Theorem 12.1 (Zorn's Lemma)**.** *Let X be a poset s.t. every chain in X has an upper bound in X. Then X has a maximal element.*

Remark. *The hypothesis implies $X \neq \emptyset$.*

Prop 12.3. *Any finitely generated nontrivial group has maximal subgroup.*

Proof. Let X be the poset of proper subgroup ordered by inclusion. $X \neq \emptyset$ since $G \neq \{1\}$. Let $C = \{H_\alpha\}_{\alpha \in I}$ be a chain. Let $H = \bigcup_{\alpha \in I} H_\alpha$ then $H \leq G$ (uses C is a chain). □

13 Oct 11

13.1 Zorn's Lemma Cont

Def. *Let R be a ring and M a left R-module. A* ***basis*** *of M is a subset that is linearly independent and generating.*

Prop 13.1. *Let R be a division ring (ring in which every nonzero element is invertible). Then any non-trivial R-module has a basis.*

Proof. Let X be the poset of linearly independent subsets of M ordered by inclusion. Let C be a chain and note that $c = \bigcup_{s \in C} s$ is an upper bound in X and is linearly independent since linearly independence only covers finite linear sums. Apply Zorn to get maximal linearly independent set B. Note that this also generates M since if $m \notin M$ then $B \cup \{m\}$ is linear independent, contradicting the maximal linear independent set B. $\square$

Remark. *If every left module over R has a basis, then R is a division ring.*

Remark. *Division rings arise alongside projective geometries by adding Desargues axiom.*

Prop 13.2. *Let R be a non-trivial ring with identity 1 ie $0 \neq 1 in R$. Then R has a maximal ideal (left, right, or two-sided).*

Proof. X poset of proper (left) ideals of R. If $C = \{I_\alpha\}_{\alpha \in A}$ is a chain in X, then $\bigcup_{\alpha \in A} I_\alpha$ is a (left) ideal. I is proper since if $I = R$ then $1 \in I \implies 1 \in I_\alpha$ so $R \subseteq I_\alpha$, a contradiction. Apply Zorn's Lemma. $\square$

Def. *A poset is* ***well-ordered*** *if it is totally ordered and every nonempty subset S has a minimum $m \in S$.*

Prop 13.3 (lTransfinite Induction)**.** *Let A be a well-ordered poset and P be a property on A, $P : A \to \{T, F\}$. Suppose for any $b \in A$ that if P holds for all $a \prec b$ then it holds for n, or that P is inductive. Then P holds for all elements of A.*

Proof. Otherwise $\{x \in A | P(x) = F\}$ has minimum b, but P is inductive so P holds for b. Contradiction. $\square$

Theorem 13.1 (Axiom of Choice)**.** *Let X be a set and $\{A_\alpha\}_{\alpha \in X}$ a family of nonempty sets. Then $\prod_{\alpha \in X} A_\alpha \neq \emptyset$. In other words, we have a function $f : X \to \bigcup_{\alpha \in X} A_\alpha$ s.t. $f(\alpha) \in A_\alpha$ for all α. Such an f is called a* ***choice function****.*

Proof. (Zorn's Lemma) Suppose X has no maximal element. Choose for each $x \in X$ an x^+ s.t. $x \prec x^+$. This is possible by assumption that X has no maximal element and by Axiom of Choice. For each chain C, we choose upper bound $u(C) \in X$, again by hypothesis and Axiom of Choice.

Let A be a well-ordered set. We define a sequence $\{x_a\}_{a \in A}$ in X s.t. if $a < b$ in A then $x_a \prec x_b$ in X. We do this by transfinite induction. Suppose we have defined x_a for all $a < b$. We have an increasing $\{x_a\}_{a<b}$ in X. This is a chain in X, so we can define $x_b = u(\{x_a\}_{a<b})^+$. Then $x_b > u(\{x_a\}_{a<b})$ in X. By transfinite induction, we have $\{x_a\}_{a \in A}$ strictly increasing in X. This contradicts **Hartog's Lemma**. □

Lemma (Hartog's Lemma)**.** *Given a set X, there exists a well-ordered set A s.t. there is no injection $A \hookrightarrow X$.*

14 Oct 22

14.1 Rings

Def. *A ring $(R, +, 0, \cdot, 1)$ consists of*

- *an abelian group $(R, +, 0)$*
- *a Monoid $(R, \cdot, 1)$.*

s.t.

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(a + b) \cdot c = a \cdot c + b \cdot c$

Ex.

1. $\mathbb{Z}$ *and* $\mathbb{Z}_n$.
2. $R[x]$ *the ring of polynomials*
3. $M_n(R)$ *the set of $n \times n$ matrices with entries in R.*
4. $\mathbb{R}^X$ *the ring of function $X \to R$ with $(f + g)(x) = f(x) + g(x), (f \cdot g)(x) = f(x) \cdot g(x)$.*

Remark.

1. *The inverse of a under addition is $-a$ (**opposite** of a). The inverse of a multiplicatively is a^{-1} (**inverse**). The set of **invertible** elements in $(R, \cdot, 1)$ is $R^{\times}$ implies that $(R^{\times}, \cdot, 1)$ is a group.*

2. *For any $a \in R$ $a \cdot 0 = 0 \cdot a = 0$ (absorption).*

3. *If $0 = 1$ then R is the zero ring (only 0).*

4. *An element $z \in R$ is a **zero divisor** if there is a w s.t. $zw = 0$ or $wz = 0$. Let R^z be the set of zero-divisors.*

5. *$0 \in R^z, 1 \in R^{\times}$ and $R^{\times} \cap R^z = \emptyset$.*

Ex.

1. *$R = \mathbb{Z} \implies R^z = \{0\}, R^{\times} = \{\pm 1\}$.*

2. *$R = M_n(\mathbb{F})$ where $\mathbb{F}$ is a field. $R^{\times} = GL_n(\mathbb{F})$. $R^z = M_n(\mathbb{F}) \setminus GL_n(\mathbb{F})$.*

Def. *A nontrivial ring R is a **domain** if $R^z = \{0\}$. A **division ring** is $R^{\times} = R \setminus \{0\}$ (also known as **skew-field**). It is an **integral domain** if it is commutative domain. It is a **field** if it is a commutative division ring.*

Def. *Let R be a ring. A subset $S \subseteq R$ is a **subring** if it is both a subgroup of $(R, +, 0)$ the addition group and a submonoid of $(R, \circ, 1)$. In this case, S is a ring.*

Def. *Let R_1, R_2 be rings. $\varphi : R_1 \to R_2$ is a **morphism** of rings if it is a morphism of the groups $(R_1, +, 0) \to (R_2, +, 0)$ and the monoids $(R_1, \cdot, 1) \to (R_2, \cdot, 1)$ and $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ and $\varphi(1) = 1$.*

Def. *Let R be a ring and $I \subseteq R$ a subgroup if $(R, +, 0)$. I is a **left ideal** if $\forall a \in R, x \in I, ax \in I$. Similarly we can define right and 2 sided ideals.*

Let I be a 2-sided ideal. Write $a \equiv b \pmod{I}$ if $a - b \in I$. This is an equivalent relation and it is compatible with both $+$ and $\cdot$. We can define R/I as the set of equivalence classes. It is also a ring.

Ex. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

Prop 14.1 (First isomorphism Theorem for Rings)**.** *Let $\varphi : R \to R'$ be a morphism of rings. $\ker(\varphi) = \{x \in R : \varphi(x) = 0\}$. It is a 2-sided ideal of R. The image φ is not an ideal, but is a subring of R'. $R/\ker\varphi \cong \operatorname{im}\varphi$ given by $\overline{a} \to \varphi(a)$.*

Ex. $\varphi : \mathbb{R}[x] \to \mathbb{C}$ *by* $\varphi(p(x)) = p(i)$. φ *is a surjective ring homomorphism.* $\ker(\varphi) = (x^2 + 1)$, *where the parenthesis is the generation of the ideal.* $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Prop 14.2 (Other Isomorphism Theorems for Rings)**.** *Let R be a ring*

1. *S a subring and I is a 2-sided ideal. Then*
   (a) *$S + I$ is a subring of R.*
   (b) *$S \cap I$ is a 2-sided ideal of R.*
   (c) $(S + I)/I \cong S/S \cap I$.
2. *Let I, J be 2-sided ideals of R w/ $I \subseteq J$. Then*
   (a) *J/I is a 2-sided ideal of R/I.*
   (b) $\frac{R/I}{J/I} \cong R/J$.
3. *Let I be a 2-sided ideal of R there is a bijective correspondence between 2-sided ideals J of R containing I and 2-sided ideals of R/I. The same holds for left and right ideals.*

Def. *Let R be a nontrivial ring R. A* ***proper ideal*** *I (left, right, 2-sided) is* ***maximal*** *if it is a maximal element of the poset of ideals under inclusion.*

Prop 14.3. *A nontrivial ring has a maximal ideal $(L, R, 2)$. More generally, any proper ideal is contained in a maximal ideal.*

Prop 14.4. *Let R be a nontrivial commutative ring. The following are equivalent*

1. *R is a field*
2. *$\{0\}$ is the only proper ideal*
3. *$\{0\}$ is maximal ideal*

Proof. For (1) $\to$ (2). If $I \neq \{0\}$, take $a \in I$, take $a \in I$, $a \neq 0$ which implies $a \in R^{\times} \implies 1 = a^{-1} \cdot a \in I \implies b = b \cdot 1 \in I$ for all b. □

Corrollary. *Let I be an ideal of commutative ring R. I is maximal iff R/I is a field.*

Proof. Use fourth isomorphism thm. □

Prop 14.5. *Let R be a nontrivial ring. The following are equivalent*

1. *R is a division ring.*
2. *$\{0\}$ is the only proper left or right ideal.*
3. *$\{0\}$ is a maximal left or right ideal.*

Def. *A ring is* ***simple*** *if it is nontrivial and $\{0\}$ is the only proper 2-sided ideal.*

Remark. *A division ring is a simple ring, but not backwards.*

Ex. *$M_n(\mathbb{F})$ is simple. It is not a division ring if $n > 1$. This is found in HW 8, Ex 15.*

Def. *Let I and J be 2-sided ideals of R. $I + J = \{a + b\}$ and $I \cdot J = \{\sum_{i=1}^{m} a_i b_i\}$. Then $I + J, I \cap J, I \cdot J$ are ideals.*

$$\begin{tikzcd}
 & I + J \arrow[dl, dash] \arrow[dr, dash] & \\
I \arrow[dr, dash] & & J \arrow[dl, dash] \\
 & I \cap J \arrow[dl, dash] \arrow[dr, dash] & \\
I \cdot J & & J \cdot I
\end{tikzcd}$$

Def. *Two 2-sided ideals I and J are* ***comaximal*** *if $I + J = R$. Equiv no proper ideal contains both I and J or no maximal ideal.*

Theorem 14.1 (CRT)**.** *Let I and J be comaximal 2-sided ideals of R. Let $\varphi : R \to R/I \times R/J$ be $\varphi(a) = (aI, aJ)$.*

1. *φ is surjective morphism of rings and $\ker(\varphi) = I \cap J$.*
2. *$R/(I \cap J) \cong R/I \times R/J$*
3. *$I \cap J = I \cdot J + J \cdot I$*

15 Oct 24

15.1 Rings cont.

Theorem 15.1 (CRT)**.** *I, J comaximal ideals in R with $\varphi : R \to R/I \times R/J$ given by $a \to (\overline{a}, \overline{a})$. Then*

1. *φ is onto and $\ker \varphi = I \cap J$.*
2. *$R/(I \cap J) \cong R/I \times R/J$.*
3. *$I \cap J = IJ + JI$.*

Proof.

1. Given $a, b \in R$ want $x \in R$ s.t. $\overline{x} = \overline{a} \pmod I$ and $\overline{x} + \overline{b} \pmod J$. Since $I + J = R$, then $1 = i + j$ for $i \in I, j \in J$. Tkae $x = bi + aj$.
2. Later.
3. Take $x \in I \cap J$. Then $x = xe + xf \in IJ + JI$.

$\square$

Ex.

1. *Let $R = \mathbb{Z}$. $n\mathbb{Z}$ is an ideal and are the only ideals. $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$ so the poset of ideals of $\mathbb{Z}$ is anti-isomorphic to the poset of $\mathbb{N}$ under divisibility. Then we see that*

$$\begin{tikzcd}[column sep=small]
 & I+J \arrow[dl, no head] \arrow[dr, no head] & & & & \gcd n, m \arrow[dl, no head] \arrow[dr, no head] & \\
I \arrow[dr, no head] & & J \arrow[dl, no head] & \leftrightarrow & n \arrow[dr, no head] & & m \arrow[dl, no head] \\
 & I \cap J \arrow[d, no head] & & & & \mathrm{lcm}(n, m) \arrow[d, no head] & \\
 & IJ & & & & nm &
\end{tikzcd}$$

By CRT if $\gcd(n, m) = 1$ then $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Explicitly, given $a, b \in \mathbb{Z}$ with $x \equiv a \pmod n$ and $x \equiv b \pmod m$ has a solution, unique modulo mn.

2. $R = \mathbb{F}^{\times}$ *(X a set, $\mathbb{F}$ a field). HW7 shows that every ideal is of the form* $\mathcal{I}(S)$. *For a unique $S \subseteq X$, where* $\mathcal{I}(S) = \{f \in \mathbb{F}^{\times} : f|_S \equiv 0\}$. *Also* $\mathbb{F}^{\times}/\mathcal{I}(S) \cong \mathbb{F}^S$. *The poset of ideals of R is anti-isomorphic to the poset of subsets of X (under inclusion).*

$$\begin{tikzcd}[arrows=dash]
& R \arrow[d] & & & \emptyset \arrow[d] & \\
& I+J \arrow[dl] \arrow[dr] & & & S \cap T \arrow[dl] \arrow[dr] & \\
I \arrow[dr] & & J \arrow[dl] \arrow[r, phantom, "\leftrightarrow"] & S \arrow[dr] & & T \arrow[dl] \\
& I \cap J \arrow[d] & & & S \cup T \arrow[d] & \\
& IJ & & & S \cup T &
\end{tikzcd}$$

where $I = \mathcal{I}(S), J = \mathcal{I}(T)$. *BY CRT, if* $S \cap T = \emptyset$ *then* $\mathbb{F}^{\times}/\mathcal{I}(S) \cap \mathcal{I}(T) \cong \mathbb{F}^{\times}/\mathcal{I}(S) \times \mathbb{F}^{\times}/\mathcal{I}(T)$ *is given by* $\mathbb{F}^{S \cup T} \cong \mathbb{F}^S \times \mathbb{F}^T$.

15.2 Noetherian Rings

Def. *A poset satisfies the* ***ascending chain condition*** *(ACC) if every countable ascending chain stabilizers ie* $x_0 \leq x_1, \cdots \implies \exists N$ *s.t.* $x_N = x_n \; \forall n \geq N$.

Prop 15.1. *A poset X satisfies ACC iff any nonempty subset S of X has a maximal element. (there is a $m \in S$ s.t. if $m < x$ then $x \notin S$).*

Proof. For forward, suppose $S \neq \emptyset$ has no max element. $S \neq \emptyset \implies \exists x_0 \in S \implies x_0$ is not maximal. This implies there exists $x_1 \in S, x_0 < x_1$. By induction, we can construct a sequence $x_n \in S$ for $n \in \mathbb{N}$ s.t. $x_{)} < x_1 \ldots,$ which is a contradiction. This uses the axiom of countable choice.

For the backwards, given a chain $x_0 \leq x_1 \ldots$ let $S = \{x_0, x_1 \ldots\}$ and S has a maximal element which is x_N. This is the definition of ACC. □

Def. *A ring R is left noetherian if the poset of left ideals satisfies ACC (similarly right noetherian for right ideals).*

Remark. *Exist rings R that are left noetherian but not right noetherian. Maybe it could be both or neither.*

Prop 15.2. *Any quotient of a left noetherian ring is also left noetherian.*

Def. *Given a subset A in a ring R, the left ideal* ***generated*** *by A is $RA = \{\sum_{i \in F} r_i a_i : F$ finite $, a_i \in A, r_i \in R, \forall i \in F\}$ A left ideal I is* ***finitely generated*** *if there is a finite $A \subseteq R$ s.t. $I = RA$. I is* ***principal*** *if there is an $a \in R$ s.t. $I = R\{a\}$.*

Prop 15.3. *A ring is left noetherian $\iff$ every left ideal is finitely generated.*

Proof. For forward, let I be a left ideal $\mathcal{F} = \{RA : A \subseteq I, \text{finite}\}$. $\mathcal{F}$ has a maximal element RA. We claim that $RA = I$. If note, then there is an $x \in I$ s.t. $x \notin RA$. Let $A' = A \cup \{x\}$ still finite and $A' \in \mathcal{F}$ with $RA \subseteq RA'$ so $x \in RA$ which is a contradiction.

For backwards, let $I_0 \subseteq I_1 \ldots$ be an ascending chain of left ideals. Let $I = \bigcup_{n \geq 0} I_n$. Then I is an ideal which implies I is finitely generated, $I = R\{a_1, \ldots, a_k\}$ which implies $a_i \in I_{n_i}$ for all $i \in [n]$. Let $N = \max\{n_1, \ldots, n_k\}$ then $a_i \in I_N$ so $I = I_N$. □

Ex.

1. *Any division ring is left noetherian.*
2. *Any PID is noetherian (principal implies finitely generated)*
3. *$R[x_1, x_2, \ldots,]$ polynomials in countably many variables is not left noetherian. By $R[x_1] \subset R[x_1, x_2] \ldots$*
4. *$R^{\times}$ (R a ring, X an infinite set). Not left or right noetherian.*

Remark. *$R[x]$ is not commutative. R commutative iff $R[x]$ is commutative. This is only the case when R is commutative.*

Theorem 15.2 (Hilbert's Basis Theorem)**.** *If R is left noetherian then $R[x]$ is left noetherian*

Proof. Let I be a left ideal. Suppose I is not finitely generated. In particular, $I \neq \{0\}$. Let $f_0 \in I$ be a polynomial of minimal degree. Now $I \neq R[x]\{f_0\}$ let $f_1 \in I \setminus R[x]\{f_0\}$ of minimal degree. Note that $\deg f_0 \leq \deg f_1$. Choose $f_n \in I \setminus R[x]\{f_0, \ldots, f_{n-1}\}$ of minimal degree. Then $\deg f_{n-1} \leq \deg f_n$. Let $d_n = \deg f_n$ and let the leading term be $a_{\deg f} x^{\deg f}$. Consider the chain of left ideals in R given by $R\{a_0\} \subseteq R\{a_0, a_1\} \ldots$. R left noetherian implies this chain stabilizes. $\exists N \in \mathbb{N}$ s.t. $a_n \in R\{a_0, a_1 \ldots, a_N\}$ for all $n \geq N$. in particular $a_{N+1} = \sum_{i=1}^{N} r_i a_i$ for some $r_i \in R$. Consider $g = \sum_{i=1}^{N} r_i f_i x^{d_{N+1} - d_i}$. The leading term of g is the same as that of f_{N+1}, so $\deg(f_{N+1} - g) < \deg(f_{N+1})$ and note that $g \in R[x]\{f_1, \ldots, f_N\}$ but this contradicts the assumption that $\deg(f_{N+1})$ is the minimal degree polynomial of our set. □

16 Oct 29

16.1 Modules

Def. *Let R be a ring. A left R-module is an abelian group $(M, +, 0)$ with a map $R \times M \to M$, $(a, m) \to a \cdot m$ s.t.*

(i) $a \cdot (b \cdot m) = ab \cdot m$. *This also gives us* $1 \cdot m = m$.

(ii) $a \cdot (m + n) = a \cdot m + a \cdot n$.

(iii) $(a + b) \cdot m = a \cdot m + b \cdot n$.

Remark.

1. *(i) (i) occurs when $(R, \cdot, 1)$ acts on M as a set.*
   (ii) (ii) occurs when the action is by endomorphism of $(M, +, 0)$.
   (iii) (iii) means that the map $R \times M \to M$ is biadditive.

2. *Replace $m \in M$ by $c \in R$. The axioms hold. So $M = R$ is a left R-module with $a \cdot c = ac$. This is the* ***standard*** *R*

3. *The endomorphisms of M is a ring under $(f + g)(m) = f(m) + g(m)$ and $(f \circ g)(m) = f(g(m))$. A map $R \times M \to M$ gives rise to $R \xrightarrow{\ell} M^M = \{f : M \to M\}$ given by $\ell(a) : M \to M, \ell(a)(m) = a \cdot m$. We see that properties $(i), (ii), (iii)$ hold. Given an abelian group M, a left R-module structure on M is* ***equivalent*** *to a ring homomorphism $R \to \mathrm{End}_{\mathbb{Z}}(M)$.*

Prop 16.1.

1. *Let R be a ring. There exists a unique ring homomorphism $\mathbb{Z} \to R$. $\mathbb{Z}$ is the initial ring.*

2. *Let M be an abelian group. There exists a unique $\mathbb{Z}$-module structure on M.*

Proof.

1. Define $\varphi : \mathbb{Z} \to R$ by $\varphi(0) = 0, \varphi(1) = 1$ and $\varphi(n) = \varphi(1 + \cdots + 1) = 1 + \cdots + 1$ for positive n and $\varphi(n) = -(\varphi(-n))$ for negative n. Note that the addition is actually in n for the last term in the first equality chain.

2. There is a unique ring homomorphism $\mathbb{Z} \to \mathrm{End}_{\mathbb{Z}}(M)$The $\mathbb{Z}$ mod structure is $n \cdot m = m + m \cdots + m$ n times.

$\square$

Def. *Let M be a left R-module. A subset $N \subseteq M$ is a* ***submodule*** *if it is a subgroup of $(M, +, 0)$ and $a \cdot n \in N$ $\forall a \in R, n \in N$. In this case, N is a left R-module $(N \leq M)$ and M/N is a left R-module with $a \cdot \overline{m} = \overline{a \cdot m}$.*

Ex.

1. *Let $M = R$ the standard left R module. The submodules of M are the left ideal of R.*

2. *Let $R = \mathbb{Z}$ and let M be an abelian group. Then the submodule of M are the subgroups of M.*

Def. *Let M be a left R-module and $A \subseteq M$ be a subset. The R-submodule* ***generated*** *by A is $RA = \{\sum_F r_i a_i : F \text{ finite}, i \in F\}$. RA is the smallest submodule of M that has A. A module M is* ***finitely generated*** *if there is a finite $A \subseteq M$ s.t. $M = RA$. It is* ***cyclic*** *if it is generated by a single element.*

Ex.

1. *A submodule of $M = R$ are left ideals of R. Finitely generated submodules are finitely generated left ideals. Cyclic submodules are principal left ideals.*

2. *$\mathbb{Z}$-modules are abelian groups. Finitely generated $\mathbb{Z}$-modules are finitely generated abelian groups. Cyclic $\mathbb{Z}$-modules are cyclic groups.*

Def. *Let M and N be left R-modules. A homomorphism is a function $f : M \to N$ s.t. $f(m+n) = f(m) + f(n)$ and $f(a \cdot m) = a \cdot f(m)$.*

16.2 Products and sums

Def. *Let I be a set and $\{M_i\}_{i \in I}$ be a collection of left R-modules. On the Cartesian product $\prod_{i \in I} M_i$, define $(m_i)_{i \in I} + (m_i')_{i \in I}$ and $a \cdot (m_i)_{i \in I} = (a \cdot m_i)_{i \in I}$. Then $\prod_{i \in I} M_i$ is a left R-module called the* ***direct product*** *of $\{M_i\}$. Let $\bigoplus_{i \in I} M_i$ be the subset of $\prod_{i \in I} M_i$ consisting of $(m_i)_{i \in I}$ of* ***finite support:*** *$\{i \in I : m_i \neq 0\}$ is finite. Then $\bigoplus_{i \in I} M_i \leq \prod_{i \in I} M_i$. The left R-module $\bigoplus_{i \in I} M_i$ is the* ***direct sum*** *of $\{M_i\}$. If I is finite then notice they are equals.*

For each $j \in I$ there are homomorphisms of the R-modules given by $\pi_j : \prod_{i \in I} M_i \to M_j$ by projection $\pi_j((m_i)_{i \in I}) = m_j$ and $\sigma_j : M_j \to \bigoplus_{i \in} M_i, \sigma_j(m) = (m_i)_{i \in I}$ with $m_i = m$ if $i = j$ and 0 if not.

Prop 16.2. *Let $\{M_i\}_{i\in I}$ be a collection of left R-modules. let M be another left R-module.*

1. *For each $j \in I$ let $\varphi_j : M \to M_j$ be a homomorphism of R-modules. Then there exists a unique morphism of R-modules $\varphi : M \to \prod_{i\in I} M_i$ s.t.*

$$\begin{tikzcd} M \arrow[r, dotted, "\varphi"] \arrow[dr, "\varphi_j"'] & \prod_{i\in I} M_i \arrow[d, "\pi_j"] \\ & M_j \end{tikzcd}$$

2. *For each $j \in I$, let $\psi_j : M_j \to M$ be a homomorphism of R-modules. Then exists unique morphism of R-modules $\psi : \bigoplus_{i\in I} M_i \to M$ s.t.*

$$\begin{tikzcd} \bigoplus_{i\in I} M_i \arrow[r, dotted, "\psi"] & M \\ M_j \arrow[u, "\sigma_j"] \arrow[ur, "\psi_j"] & \end{tikzcd}$$

Proof.

1. Define $\varphi(m) = (\varphi_i(m))_{i\in M}$.
2. Define $\psi((m_i)_{i\in I}) = \sum_{i\in I} \psi_i(m_i)$ and since the preimage has finite support the map is well defined.

□

Remark.

General Category	*R-modules*	*groups*	*sets*
Product	*Direct Product*	*Direct Product*	*Cartesian Product*
Coproduct	*Direct Sum*	*Free product*	*Disjoint Union*

Ex. *Let $(X, \leq)$ be a poset. Define a category φ_x where objects are the elements of X and given $x, y \in X$ there exists a unique homomorphism $x \to y$ if $x \leq y$. The product of x and y exists iff $x \vee y$ exists and a coproduct if $x \wedge y$.*

17 Oct 29

17.1 Noetherian Modules

Def. *A left R-module os Noetherian if the poset of submodules satisfies ACC. IE every nonempty set of submodules has a maximal element.*

Remark. *R is left Noetherian iff it is noetherian as a left R-module.*

Prop 17.1. *A left R-module M is Noetherian iff every R-submodule is finitely generated. In particular it is itself finitely generated.*

Prop 17.2. *Let M be a left R-module and $N \leq M$. Then M is Noetherian iff N and M/N are Noetherian.*

Proof. List from N to M/N. $\square$

Prop 17.3. *Let $\{M_i\}_{i\in I}$ be Noetherian left R-modules. I finite, then $\bigoplus_{i\in I} M_i$ is Noetherian.*

Proof. By induction, we examine $I = \{1, 2\}$. Note that $M_1 \leq M$ and $M/M_1 \cong M_2$ and use the previous proposition. $\square$

Prop 17.4. *Let R be left Noetherian and M a left R-module. If M is finitely generated, then M is Noetherian.*

Proof. $M = R\{x_1, \ldots, x_k\}$. $R^k \to M$ with $e_j \to x_j$ is a surjection. So M is a quotient of R^k and R^k is Noetherian because it is finite direct sum of Noetherian modules. $\square$

Remark. *If R arbitrary and M finitely generated, then not every submodule of M is necessarily finitely generated. For example, if R is not Noetherian then $R \leq M$ is a submodule that is not finitely generated.*

17.2 Free Modules

Lemma. *Recall the standard left R-module R under left multiplication. Let M be any left R-module and any $m \in M$ then $\exists!$ morphism of left R-modules $\varphi : R \to M$ s.t. $\varphi(1) = m$.*

Proof. $\varphi(a) = a \cdot \varphi(1) = a \cdot m$. $\square$

Def. *Let I be a set. For each $i \in I$, let $M_i = R$ the standard left R-module. The module $R^{(I)} := \bigoplus_{i\in I} M_i$ is the **free left R-module** on the set I. Let $e_j \in R^{(I)}$ be the I-tuple in $R^{(I)}$ with j component equal to 1, 0 elsewhere for all $(j \in I)$.*

Remark. *$R^I = \prod_{i \in I} M_i$ is different*

Prop 17.5 (UP of Free Module)**.** *Let I be a set, M a left R-module. let $\{m_i\}_{i \in I}$ be a collection of elements in M. Then $\exists!$ morphism of R-modules $\varphi : R^{(I)} \to M$ s.t. $\varphi(e_i) = m_i$.*

$$\begin{tikzcd} I \arrow[r] \arrow[dr] & R^{(I)} \arrow[d, dotted, "\varphi"] \\ & M \end{tikzcd}$$

by $i \to e_i \to m_i$.

Remark. *Use the Lemma to define a morphism $\varphi_i : R \to M_i$ s.t. $\varphi_i(1) = m_i$. By UP of direct sum, exists a unique morphism φ*

$$\begin{tikzcd} M_i \arrow[r, "\sigma_i"] \arrow[dr, "\varphi_i"'] & R^{(I)} \arrow[d, dotted, "\varphi"] \\ & M \end{tikzcd}$$

$m_i = \varphi_i(1) = \varphi\sigma_i(1) = \varphi(e_i)$.

Def. *Let M be a left R-module and $S \subseteq M$ a subset. S is **linearly independent** if $\sum_{i \in F} a_i m_i = 0$ with F finite $a_i \in R, m_i \in S$ implies $a_i = 0$ for all $i \in F$. S **generates** M if for any $m \in M$ there exists F finite, $a_i \in R_i, m_i \in S$ for $i \in F$. s.t. $m = \sum_{i \in F} a_i m_i$.*

Prop 17.6. *Let I be a set. Then*

1. *The set $\{e_i\}_{i \in I}$ is a basis of $R^{(I)}$.*
2. *Suppose M is a left R-module with basis I.. Then $M \cong R^{(I)}$.*

Proof.

1. For any $(a_i)_{i \in I} \in R^{(I)}$ claim $(a_i)_{i \in I} = \sum_{i \in I} a_i \varphi_i$. Part 2 follows.

□

17.3 Tensor Products

Def. *Let R be a* ***commutative ring****. This implies left R-modules are right R-modules. Note that left R-modules aren't necessarily right R-modules since $(m \cdot a) \cdot b = ba \cdot m \neq ab \cdot m$. Let M and L be R-modules. A homomorphism from $M \to L$ is* ***linear map****. This set is $\mathrm{Hom}_R(M, L)$.*

Let N be another R-module. A function $\beta : M \times N \to L$ is ***bilinear*** *if*

(i) $\beta(m + m', n) = \beta(m, n) + \beta(m', n)$.

(ii) $\beta(m, n + n') = \beta(m, n) = \beta(m, m')$.

(iii) $\beta(am, n) = a\beta(m, n) = \beta(m, an)$.

The set of these is $\mathrm{Hom}_R(M, N; L)$. ***Multilinear maps*** *are defined similarly to $\mathrm{Hom}_R(M_1, \ldots, M_n; L)$.*

Ex.

1. $\mu : R \times R \to R, (a, b) \to ab$. *This is bilinear because rings are linear.*
2. *For any R-modules $R \times M \to M, (a, m) \to a \cdot m$ is bilinear.*

Remark. $\mathrm{Hom}_R(M \times N, L) \neq \mathrm{Hom}_R(M, N; L)$. *$f : M \times N \to L$ by $f((m, n) + (m', n') = f(m, n) + f(m', n')$ isn't good enough. We'll construct $M \otimes N$ s.t. $\mathrm{Hom}_R(M \otimes N, L) \cong \mathrm{Hom}_R(M, N; L)$.*

Prop 17.7 (UP of Tensor Products)**.** *Let M and N be R-modules. $\exists$ an R-module X and a bilinear map $\theta : M \times N \to X$ s.t. given any R-module L and* ***bilinear map*** *$\beta : M \times N \to L$, $\exists!$* ***linear map*** *$\widehat{\beta} : X \to L$ s.t.*

$$\begin{tikzcd} M \times N \arrow[r, "\beta"] \arrow[d, "\theta"'] & L \\ X \arrow[ur, dotted, "\widehat{\beta}"'] & \end{tikzcd}$$

Moreover, (X, θ) is unique (up to isomorphism) with this property.

Proof. Let F be the free R-module in the set $M \times N$. F has basis $\{e_{(m,n)} : m \in M, n \in N\}$. Let F' be the submodule of F generated by

- $e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}$
- $e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}$

- $e_{(am,n)} - ae_{(m,n)}$
- $e_{(m,an)} - ae_{(m,n)}$

for all $m, m' \in M, n, n' \in N, a \in R$. Let $X = F/F'$. Define $\theta : M \times N \to X$ as $M \times N \hookrightarrow F \twoheadrightarrow F/F' = X$. by $(m,n) \to e_{(m,n)} \to \overline{e_{(m,n)}} = \theta(m,n) + \theta(m',n)$. $\square$

18 Nov 5

18.1 Divisibility

Remark. *Normally we write $\langle a \rangle = Ra$. Today R will be an integral domain.*

Def. *Let $a, b \in R$. b **divides** a if $a = bc$, $c \in R$. We write $b \mid a$. a and b are **associates** if $a \mid b, b \mid a$ and we write $a \sim b$. Let $u \in R$. We say u is a **unit** if $u \mid 1$.*

Prop 18.1.

1. *u is a unit iff u is invertible iff $\langle u \rangle = R$.*
2. *$b \mid a$ iff $\langle a \rangle \subseteq \langle b \rangle$.*
3. *$a \sim b$ iff $(a) = (b)$ iff there is a unit s.t. $a = ub$.*

Def. *Let $p \in R$. Assume $p \neq 0$ and p is not a unit. p is **irreducible** if $p = ab \implies a$ or b is a unit.It is **prime** if $p \mid ab$ implies that $p \mid a$ or b.*

Prop 18.2. *p prime implies that pis irreducible.*

Prop 18.3. *Suppose $p \sim q$.*

1. *p irreducible implies that q is irreducible.*
2. *p primes implies q is prime.*

Def. *Given $a : I \to R$ by $i \to a_i$ where I is finite, their **product** $\prod_{i \in I} a_i \in R$ is well defined. If $I = \emptyset$ then this product is defined to be 1.*

Prop 18.4 (Uniqueness of Prime Factorization)**.** *Let I and J be finite sets. Let $(p_i)_{i \in I}$ and $(q_j)_{j \in J}$ be primes. Suppose $\prod_{i \in I} p_i \sim \prod_{j \in J} q_j$. Then there exists a bijection $\sigma : I \to J$ s.t. $p_i \sim q_{\sigma(i)}$.*

Proof. Induction on $|I|$. If $|I| = 0$ we have $1 \sim \prod_{j \in J} q_j$. If $|J| \neq 0$ that implies there is a $j \in J$ s.t. $q_j \mid 1$. Suppose $|I| \geq 1 \implies \exists i_0 \in I \implies p_{i_0} \mid \prod_{i \in I} p_i = u \prod_{j \in J} q_j$ where u is a unit. p_{i_0} is a prime $\implies p_{i_0} \mid q_{j_0}$, some $j_0 \in J \implies q_{j_0} = p_{i_0} c, c \in R$. q_{j_0} irreducible and p_{i_0} not a unit implies that c is a unit so $p_{i_0} \sim q_{j_0}$. We have that $\prod_{i \in I} p_i = u \prod_{j \in J} q_j \implies \prod_{i \in I, i \neq i_0} p_i = u' \prod j \in J : j \neq j_0 q_j \sim \prod_{j \in J, j \neq j_0} q_j$. By induction hypothesis, we just define the σ for the other elements and define $\sigma(i_0) = j_0$. □

Prop 18.5 (Existence of Irreducible Factorization)**.** *Let R be Noetherian. Let $a \in R, a \neq 0$. Then $\exists$ a finite set I and irreducibles $(p_i)_{i \in I}$ s.t. $a \sim \prod_{i \in I} p_i$.*

Proof. Suppose not. Let $\mathcal{F} = \{(x) : x \neq 0, x \not\sim \text{ finite product of irreducibles}\}$. Pick a maximal element element $(x) \in \mathcal{F}$. x is not a unit and it is not irreducible, so it has an irreducible factorization. $x = yz$ where yz are not units. Both y and z. Also $y, z \neq 0$. Note that $(y), (z) \notin \mathcal{F}$ and we are done since we can find irreducible factorizations. □

18.2 Unique Factorization Domains

Prop 18.6.

1. *Every $a \in R, a \neq 0$ and non unit admits a irreducible factorization.*
2. *Any irreducible factorization is unique up reordering and units.*
3. *Every irreducible is prime*

Then $(1) + (2) \iff (1) + (3)$.

Proof. ($\Leftarrow$) (3) implies primes are irreducible and unique factorization for prime factors so (2) holds.

($\Rightarrow$) Let $p \in R$ be irreducible. Suppose $p \mid ab$. WANT $P \mid a$ or $p \mid b$ which implies that $ab = pc \implies c \neq 0$. Can factor each into irreducible $a \sim \prod_{iinI} p_i, b \sim \prod_{j \in J} q_j, c = \prod_{h \in H} r_h$. Then $\prod p_I \cdot \prod q_j \sim p \prod r_h$. By (2) we may assume that $p \sim p_i$ then $p \mid a$. □

Def. *An integral domain R is a **UFD** if $(1) + (2)$ or $(1) + (3)$ hold.*

Remark. *We saw that Noetherian implies there exists irreducible factor. However, there are UFDs that are not Noetherian ie $\mathbb{F}[x_1, x_2, \ldots]$ is a UFD (non trivial) but is not Noetherian. There are also Noetherian domains that are not UFD ie $\mathbb{Z}[\sqrt{-3}]$.*

Prop 18.7. *An integral domain is a UFD iff the (3) + (4) holds. where 4 is that principal ideals satisfy ACC.*

Proof. Same proof as in Noetherian Case gives (4) $\implies$ (1). Forward is left as exercise. $\square$

18.3 Principal Ideal Domains

Def. *An integral domain is a PID if every ideal is principal.*

Lemma. *R an integral domain. $p \in R$. p is prime iff (p) is a prime ideal. p is irreducible iff (p) is maximal among the principal ideals.*

Corrollary. *$PID \implies UFD$.*

Proof. $PID \implies$ noetherian $\implies$ (4). If p is irreducible then (p) is a maximal ideal so (p) is prime so p prime, so we have (3). $\square$

Def. *Let R be an integral domain. A* ***Euclidean Norm*** *is a function $\delta : R \setminus \{0\} \to \mathbb{N}$ s.t. for all $a \in R, b \in R \setminus \{0\}$ then there exists $q, r \in R$ with $a = bq + r$ and $\delta(r) < \delta(b)$ when $r \neq 0$.*

Def. *R is a ED if it posses a Euclidean Norm.*

Prop 18.8. *$ED \implies PID$.*

Ex.

- *$\mathbb{Z}$ is ED with $\delta(a) = |a|$.*
- *If $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a ED with $\delta(p(x)) = \deg p(x)$.*
- *$\mathbb{Z}[i]$ is a ED with $\delta(z) = |z|^2$.*

19 Nov 7

19.1 Integrality

Def. *Let $R \subseteq S$ be an integral domain. We say $\alpha \in S$ is* ***integral*** *over R if $\exists$ a monic polynomial $p(x) \in R[x]$ s.t. $p(\alpha) = 0$.*

Remark. *$\alpha \in R$ implies that α is a root of $x - \alpha$ so α is integral over R.*

Ex. *$\sqrt{2}$ is a zero of $x^2 - 2 \in \mathbb{Z}[x]$.*

Def. *Let R be an integral domain and F its field of fractions. The* ***integral closure*** *of R is $\overline{R} = \{\alpha \in F, \alpha \text{ integral over } R\}$. $R \subseteq \overline{R} \subseteq F$. We say R is* ***integrally closed*** *if $R = \overline{R}$.*

Ex. *$\mathbb{Z}$ is integrally closed. Let $\alpha \in \mathbb{Q}$ with $p(x) \in \mathbb{Z}[x]$ monic and s.t. $p(\alpha) = 0$. $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Write $\alpha = a/b$ with $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Then $p(\alpha) = 0 \implies a^n \equiv 0 \pmod{b} \implies b \mid a^n \implies b$ is a unit. In particular $\alpha \in \mathbb{Z}$.*

Corrollary. *$\sqrt{2} \notin \mathbb{Q}$.*

Prop 19.1. *Any UFD is integrally closed.*

Proof. Same proof as before, using properties of gcds that hold in all UFDs. □

Ex. *Consider $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Q}(\sqrt{-3})$. They are subrings of $\mathbb{C}$. $\mathbb{Q}(\sqrt{-3})$ is the field of fractions of $\mathbb{Z}[\sqrt{-3}]$. Let $w = \frac{-1+\sqrt{-3}}{2}$ and note that it is integral over $\mathbb{Z}[\sqrt{-3}]$ but not in it, so $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed and as such is not a UFD.*

19.2 Quadratic Integers

Def. *$\alpha \in \mathbb{C}$ is a quadratic integer if $\exists$ monic $p(x) \in \mathbb{Z}[x]$ of degree 2 s.t. $p(\alpha) = 0$.*

Def. *Given $\alpha \in \mathbb{C}$, let $Q(\alpha)$ = smallest subfield of $\mathbb{C}$ containing α and similarly $\mathbb{Z}[\alpha]$ be the smallest subring of $\mathbb{C}$ containing α. If α is a quadratic integer, then $Q(\alpha) = \{a + b\alpha : a, b \in \mathbb{Q}\}$ and $\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$. Note that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ where $d = m^2 - 4m \in \mathbb{Z}$. Write $d = k^2 D$ where D is square-free. Then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D})$.*

Let $\beta = \frac{-1+\sqrt{D}}{2} \in \mathbb{Q}(\sqrt{D}) \setminus \mathbb{Z}[\sqrt{D}]$ If $D \equiv 1 \pmod{4}$, β is integral over $\mathbb{Z}[\sqrt{D}]$ therefore this case is not integrally closed and not a UFD.

Def. *Let $D \in \mathbb{Z}$ be square-free. The* ***ring of quadratic integers of discriminant*** *D is $\mathcal{O}(D) = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \equiv 2, 3 \pmod{4} \\ \mathbb{Z}[\frac{-1+\sqrt{D}}{2}] & D \equiv 1 \pmod{4} \end{cases}$.*

Ex. *$\mathcal{O}(-1) = \mathbb{Z}[i]$ Gaussian integers, $(-3) = \mathbb{Z}[w]$ the Eisenstein integers.*

Remark.

- *$\mathcal{O}(D)$ is integrally closed for all D (in fact it is the integral closure of$\mathbb{Z}[\sqrt{D}]$).*

- *$\mathcal{O}(D)$ is UFD iff $\mathcal{O}(D)$ is PID.*

- *For $D < 0$ $\mathcal{O}(D)$ is a UFD for finitely many values of D.*

- *For $D > 0$, $D = 10$ is the first for which $\mathcal{O}(D)$ is not a UFD. Gauss conjectured that for it is a UFD for infinitely many values of $D > 0$.*

19.3 Dedekind Domains

Def. *A Dedekind domain (DD) is an integral domain that is Noetherian, Integrally Closed, and every prime ideal is maximal.*

Remark.

- *$\mathcal{O}(D)$ is always a DD.*

- *UFD and DD iff PID.*

Remark. *Fields - ED - PID - UFD/ DD - ID is ordering with fields the simplest.*

Remark.

- *$\mathbb{Z}, \mathbb{F}[x], \mathbb{Z}[i], \mathbb{Z}[w]$ are ED.*

- *$\mathcal{O}(-19)$ PID not ED.*

- *$\mathcal{O}(-5)$ and $\mathcal{O}(10)$ are DD's not UFD.*

- *$\mathbb{Z}[x_1, \ldots, x_n]$ UFD not DD. Same for $\mathbb{Z}[x_1, x_2, \ldots]$.*

19.4 Polynomial Rings

Remark.

- *R integral domain implies that $R[x]$ is an integral domain.* $\deg(f \cdot g) = \deg(f) + \deg(g)$.

- *$f(x) \in R[x]^\times$ implies that $f(x) = u$ with u a unit in R.*

- *F field implies $F[x]$ ED implies $F[x]$ PID.*

- *R PID does not implies $R[x]$ PID. Our goal is to show that this holds for UFDs however.*

Remark. *R a UFD, F its fields of fractions. Factorization and irreducibles in $F[x]$ of in $R[x]$.*

- *If $f(x) \in R[x]$ factors in $F[x]$, then we can juggle constants to get a factorization in $R[x]$.*
- *Irreducibles in $R[x]$ are the same as those in $F[x]$ except for "obvious" differences involving constants.*

Ex. $R = \mathbb{Z}, F = \mathbb{Q}$.

1. $f(x) = 8x^2 + 2x - 15$. *It is* $(4x - 5)(2x + 3)$
2. $f = 2, g(x) = 2x + 4$. *f is irreducible in $\mathbb{Z}[x]$ but not $\mathbb{Q}[x]$ and g is irreducible in $\mathbb{Q}[x]$ but not $\mathbb{Z}[x]$.*

20 Nov 12

20.1 More Prime Factorization of UFDs

Theorem 20.1 (Gauss Lemma). *Let R be a UFD and F be its field of fractions. Let $h \in R[x]$. Suppose $\exists f(x), g(x) \in F[x]$ s.t. $h(x) = f(x)g(x)$. Then there exists $A, B \in F^\times$ s.t. $\tilde{f}(x) = Af(x) \in R[x]$ and $\tilde{g}(x) = Bg(x) \in R[x]$ and $h(x) = \tilde{f}(x)\tilde{g}(x)$.*

Ex. $h(x) = 8x^2 + 2x - 15$ *and* $h(x) = 8(x - 5/4)(x + 3/2)$ *then*$f(x) = 2x - 5/2, g(x) = 4x + 6$ *then* $\tilde{f}(x) = 4x - 5, \tilde{g}(x) = 2x + 3$.

Proof. Let d be the product of all denominators of $f(x)$ and $g(x)$ $d \in R^\times$. Then that implies that $dh(x) = f_1(x)g_1(x)$ with $f_1(x), g_1(x) \in R[x]$ and $f_1(x) = A_1 f(x), g_1(x) = B_1 g(x)$. Factor d into irreducibles (R is a UFD). We claim that if p is a prime, p/d then either p divides all coefficients of f_1 or all coefficients of g_1. Can then cancel p from both sides and proceed.

Consider $\overline{R} = R/(p)$. p prime implies that (p) is a prime ideal which implies $\overline{R}$ is an integral domain. This implies that $\overline{R}[x]$ is an integral domain and let $R[x] \to \overline{R}[x]$ by $\sum a_i x^i \to \sum \overline{a_i} x^i$. We have that $dh(x) = f_1(x)g_1(x) \implies \overline{0} = \overline{f_1}(x)\overline{g_1}(x)$ which implies that either $\overline{f_1}(x) = 0$ or $\overline{g_1}(x) = 0$ since it is an integral domain. This completes the claim and the argument. $\square$

Corrollary. *R a UFD, F is the fraction field of R. Let $h(x) \in R[x] \subseteq F[x]$. Then*

1. *Suppose* $\deg(h) = 0$. *Write* $h(x) = p \in R$. *Then* $h(x)$ *is irreducible in* $R[x]$ *iff* p *is irreducible in* R.

2. *Suppose* $\deg(h) \geq 1$. *Then* $h(x)$ *is irreducible in* $R[x]$ *iff* $h(x)$ *is irreducible in* $F[x]$ *and* $h(x)$ *is primitive.*

Remark. *Recall that* $\gcd(a, b)$ *exists for any* $a, b \in R$ *if* R *is a UFD. It is unique up to units.*

Prop 20.1. *Given* a, b *if* $d \sim \gcd(a, b)$ *can write* $a = d'a, b = db'$ *and* $\gcd(a', b') \sim 1$. *Also can speak of* $\gcd(a_1, \ldots, a_n)$.

Def. *The* ***content*** *of* $f(x)$ *is* $c(f) \sim \gcd(a_0, \ldots, a_n)$. $f(x) \in R[x] \setminus \{0\}$ *is* ***primitive*** *if* $c(f) \sim 1$. *Given any* $f(x) \in R[x] \setminus \{0\}$ *we can write* $f(x) = c(f)f_1(x)$ *where* $f_1(x)$ *is primitive.*

Ex. $(hx) = 2x + 4$ *is irreducible in* $F[x]$ *but reduces to* $2(x + 2)$ *in* $R[x]$.

Proof. Use $R[x]^\times = R^\times$.

$h(x) = c(h)h'(x)$ where $\deg(h') = \deg(h) \geq 1$ which implies that $h'(x)$ is not a unit. This implies $c(h)$ is a unit in $R[x]$ which implies that $c(h) \in R^\times$. So $h(x)$ is primitive.

Suppose we have a factorization $h(x) = f(x)g(x)$ with $f(x), g(x) \in F[x]$. By Gauss we have that $h(x) = f_1(x)g_1(x)$ where $f_1, g_1 \in R[x]$ and are multiples of f, g respectively. This implies that f_1 or $g_1 \in R[x]^\times$. and if we suppose the first holds then we get that $\deg(f_1) = 0 \implies f(x) \in F[x]^\times$.

For the converse, suppose $h(x) = f(x)g(x)$ with $f(x), g(x) \in R[x]$ which implies that $f(x), g(x) \in F[x]$ and $f(x) \in F[x]^\times, g(x) \in F[x]^\times$. Suppose that the first holds then $f(x) = u \in F6\times$. But $f(x) \in R[x]$ so $u \in R \setminus \{0\}$ .We get that $h(x) = ug(x) \implies f(x) \in R[x]^\times$. $\square$

Ex.

1. *Let* $a, b \in R, a \neq 0$ *then* $ax + b$ *is irreducible in* $R[x]$ *iff* $\gcd(a, b) \sim 1$.

2. *Let* $n \geq 0$. *We claim that* $x^n + y \in F[x, y] = F[x][y]$ *is irreducible. The proof is that as an element of* $F[x][y]$, $x^n + y$ *is of degree* 1 *and* $\gcd(x^n, 1) \sim 1$ *and we apply the above.*

Theorem 20.2. *If* R *is a UFD then* $R[x]$ *is a UFD.*

Proof. We will do existence only. Let $f(x) \in R[x] \setminus \{0\}$. Write $f(x) = c(f)f'(x)$. Since R is a UFD then $c(f) = \prod_{i \in I} p_i$ suffices to assume that $f(x)$ is primitive.

Let F be the fraction field of R. Then $F[x]$ is a PID which implies that $F[x]$ is a UFD. So we can factor in $F[x]$. $f(x) = p_1(x) \dots p_n(x)$. where each $p_i(x)$ is irreducible in $F[x]$. By Gauss we can get $\tilde{p_i}(x) \in R[x]$, which are $\sim p_i(x)$ and as such are irreducible. But $c(\tilde{p_i})/c(f) \sim 1$ so $\tilde{p_i}(x)$ primitive and are also irreducible, which is our desired factorization. $\square$

20.2 Modules over Domains

Def. *Let M be a R-module. The **rank** of M is the maximal size of linearly independent subsets of M. Denote it as* $\mathrm{rk}(M)$.

Prop 20.2. *Suppose $M \cong R^r$ with $r < \infty$.* $\mathrm{rk}(M) = r$. *and any basis of M has r elements.*

Proof. $M \subseteq F \otimes \cdots \otimes F$ where F is ff of R. We claim that if $S \subseteq M$ is a li over R then it is li over F. The proof of this is that if we have $\sum_{s \in S} a_s s = 0$ for $a_s \in F$ then we choose denominator that is multiple over all denominators. Therefore we have that $\sum_{s \in S} d a_s s = 0$ so $\mathrm{rk}(M) \leq \dim_F F^r = r$.

For the converse inequality, we note that $S = \{e_1, \dots, e_r\}$ is good enough.

For the other claim let T be a basis of M. Let $t = |T|$. Then T is li implies $t \leq \mathrm{rk}(M) = r$. By the UP of free modules $M \cong R^{(T)} = R^t$. $\mathrm{rk}(M) = t$. $\square$

21 Nov 14

21.1 Principal Modules

Remark. *Recall that for V vector space and $W \leq V$ then $V \cong W \oplus V/W$. If we choose a basis of V/W then we get this. This is not true for all modules since if $M = \mathbb{Z}, N = 2\mathbb{Z}$ then $M/N \cong \mathbb{Z}_2$ but $\mathbb{Z} \ncong 2\mathbb{Z} \oplus \mathbb{Z}_2$.*

Lemma (Free quotients split). *R a ring, M a left R-module ,$N \leq M$. Suppose M/N is free (as a left R-module). Then $M \cong N \oplus M/N$.*

Lemma. *R a PID, $I \leq R$ a non-zero ideal. Then I is free of rank* 1 *(as an R-Module).*

Proof. $I = (a)$ for some $a \in R \setminus \{0\}$. $\{a\}$ generates I and is linearly independent. $\square$

Prop 21.1. *R PID. Let M be a free module of rank r, $N \leq M$. Then N is free of rank $\leq r$.*

Proof. Assume$M = R^r$. Induct on r. If $r = 1$ then done by above. If $r \geq 2$ let $\varphi : R^r \to R$ and is equal to projection to the last element. φ is a morphism of module and is onto. Let $I = \varphi(N) \leq R$. We see that

$$\begin{array}{ccccc} \ker\varphi & \longrightarrow & R^r & \xrightarrow{\varphi} & R \\ \uparrow & & \uparrow & & \uparrow \\ N \cap \ker\varphi & \longrightarrow & N & \longrightarrow & I \end{array}$$

I ideal of R implies I is free of rank ≤ 1. $\ker\varphi = \{(a_1, \ldots, a_r) : a_r = 0\} \cong R^{r-1}$ which implies $\ker\varphi$ is free or rank $r-1$. By induction $N \cap \ker\varphi$ is free of rank $\leq r-1$. By the lemma we have that $N \cong (N \cap \ker\varphi) \oplus I \cong R^{s+t}$ where $s \leq r-1, t \leq 1$ and we are done. $\square$

Remark. *V vector space $W \leq V$. Given a basis S of V then it doesn't necessarily contain a basis of W, although there does exist one (extend the basis of W).*

Is this true for free R-modules? If $N \leq M$ with M and N free, does there exists a basis containing a basis fo N. No if we set $R = \mathbb{Z}, M = \mathbb{Z}, N = 2\mathbb{Z}$. or $R = \mathbb{Z}, M = \mathbb{Z}^2$.

Theorem 21.1 (Stacked Basis Theorem)**.** *Let R be a PID, M a free module of rank $r < \infty$. $N \leq M$. We know that N is free of rank $s \leq r$. There exists a basis $\{m_1, m_r\}$ of M and a basis $\{n_1, \ldots, n_2\}$ and elements $a_1, \ldots, a_s \in R \setminus \{0\}$ s.t. $n_i = a_i m_i$ and $a_1 \mid a_2 \mid \cdots \mid a_s$ in R.*

Lemma. *R ring, $N_i \leq M_i$ $i \in I$. Then $\bigoplus_{i\in I} M_i / \bigoplus_{i \in I} N_i \cong \bigoplus_{i\in I} M_i/N_i$.*

21.2 Structure Theorems for Finitely Generated Modules over PID

Corrollary (First Structure Theorem)**.** *R a PID, M fg R-Module. There exists $r, s \geq 0$ and elements $a_1, \ldots, a_s \in R$ with $a_i \neq 0$ and not units s.t. $M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_j)$. and $a_1 \mid a_2 \cdots \mid a_j$.*

Proof. Let $\{x_1, \ldots, x_k\}$ be a set of generators of M. Let F be the free module of rank k. Let $\{e_1, \ldots, e_k\}$ be a basis of F. Consider $\pi : F \to M$ determined by $\pi(e_i) = x_i$. Let $N = \ker \pi$. Then $M \cong F/N$. Choose a pair of stacked bases for F and N $\{m_1, \ldots, m_k\}$ for F and $\{n_1, \ldots, n_h\}$ of N where $n_i = a_i m_i : a_1 \mid a_2 \cdots \mid a_n$. This implies that $N = Rn_1 \oplus \cdots \oplus n_h$, $F = Rm_1 \oplus \cdots \oplus Rm_h \oplus \ldots Rm_k$. We get that $M \cong F/N \cong Rm_1/Rn_1 \oplus \cdots \oplus Rm_h/Rn_h \oplus \cdots \oplus Rm_k$. We have that

$$\begin{tikzcd} R \arrow[r, "\cong"] & Rm_i \\ (a_i) \arrow[r, "\cong"] \arrow[u, hook] & Rm_i \arrow[u, hook] \end{tikzcd}$$

So we have that $Rm_i/Rm_i \cong R/(a_i)$ so $M \cong R/(a_1) \oplus \cdots \oplus R/(a_h) \oplus R \oplus \cdots \oplus R$. Can remove $R/(a_i)$ if a_i is a constant and we are done. $\square$

Remark. *Given $a \in R$ a PID, $a \neq 0$ and not a unit. Then write $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Let each p_i irreducible and $p_i \not\sim p_j$. Then $\gcd(p_i^{\alpha_i}, \ldots) \sim 1$ so $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = R$. Also (a) is the sum of $(p_i^{\alpha_i})$.*

The CRT says there exists an isomorphism of rings. This map is an isomorphism of R-modules $R/(a) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k})$.

Def. *A* ***partition*** *$\lambda = (l_1, \ldots, l_k)$ is a weakly decreasing sequence of positive integers: $l_1 \geq l_2 \cdots \geq l_n \geq 1$. Given λ and an irreducible $p \in R$, let $R/p^\lambda = R/(p^{\lambda_1}) \oplus \cdots \oplus R/(p^{l_n})$.*

Corrollary (Second Structure Theorem)**.** *R a PID, M a finitely generated R module. There exists an $r \geq 0$ and irreducible $p_1, \ldots, p_k \in R$ and $\lambda_1, \ldots, \lambda_k$ partitions of various lengths s.t. $M \cong R^r \oplus R/p_1^{\lambda_1} \oplus \cdots \oplus R/p_k^{\lambda_k}$.*

Proof. By the previous corollary we have that $M \cong R^r \oplus R/(a_1) \cdots \oplus R/(a_s)$. Writing $a_s \sim p_1^{\alpha_{s1}} \ldots p_k^{\alpha_{sk}}$ and similarly for all $i \in [s]$. Examine α_{ij}, and we can have $\alpha_{ij} = \alpha_{ji}$ (square matrix). Since each p_i is irreducible and $\alpha_{si} \geq \cdots \geq \alpha_{1i} \geq 0$ by the divisibility condition on a_i. With λ_i this sequence (removing tailing zeros), we get the desired result. $R/(a_i) \cong R/(p_1^{\alpha_{i1}}) \oplus \cdots \oplus R/(p_k^{\alpha_{ik}})$ and can rearrange. $\square$

Remark. *Both theorems are existence statements. Uniqueness holds. r is the rank of the module M, and a_i are determined by M. These are the* ***invariant factors*** *of M, the irreducibles p_i and partitions λ_i are determined. The $p_i^{\alpha_{ij}}$ are the* ***elementary divisors****.*

21.3 Stacked Basis Theorem

Theorem 21.2 (Stacked Basis Theorem). *R a PID and M a free R-module with rank $r < \infty$ and $N \leq M$. There exist bases $\{m_1, \ldots, m_r\}$ of M and $\{n_1, \ldots, n_s\}$ of N (for some $0 \leq s \leq r$) and $a_1, \ldots, a_s \in R \setminus \{0\}$ s.t.*

(i) $n_i = a_i \cdot m_i$ *for all* $i \in [s]$.

(ii) $a_1 \mid a_2 \cdots \mid a_s$.

Def. *We examine the **dual modules**. Let R be a ring and M be a left R-module. $M^* = \hom_R(M, R)$ be the set of left R-module homomorphisms $\varphi : M \to R$. Then*

(1) *$M*$ is a right R-module via $(\varphi \cdot a)(x) = \varphi(x)a$ for $\varphi \in M^*, a \in R, x \in M$.*

(2) *If R commutative then $(\varphi \cdot a)(x) = \varphi(x)a = a\varphi(x) = \varphi(a \cdot x)$.*

(3) *For $x \in M$ with $\varepsilon_x : M^* \to R$ as $\varepsilon_x(\varphi) = \varphi(x)$ then ε_x is a homomorphism of right R-modules.*

(4) *M is free of rank r and $\{x_1, \ldots, x_r\}$ is a basis. For each $i \in [r]$ define $\pi_i : M \to R$ by $\pi_i\left(\sum_{j=1}^r a_j \cdot x_j\right) = a_i$. This is well defined as we have a basis. π_i is a homomorphism of left R-modules, so $\pi_i \in M^*$.*

Lemma. *$\{\pi_1, \ldots, \pi_r\}$ forms a basis of M^* (it is free). This is the dual basis of $\{x_i\}$, and we often write x_i^*.*

Proof. Obvious. Define φ as the sum of π_i and it is linearly independent by examining $\varphi(x_i)$. □

Proof of Stacked Basis. Skipped. □

22 Nov 19

22.1 Field Characteristic

Remark. *Take $\varphi : \mathbb{Z} \to F$ with $\varphi(n) = 1 + \cdots + 1$ and negative is just $\varphi(-n) = -\varphi(n)$. $\ker\varphi$ is a prime ideal and $\operatorname{im}\varphi$ is integral domain. Therefore $\ker\varphi = \{0\}$ or (p) for some prime, then $\operatorname{im}\varphi \cong \mathbb{Z}$ or $\mathbb{Z}_p$.*

Def. *Using F and φ as defined, the **characteristic** of F, denoted char F is 0 if $\operatorname{im}\varphi \cong \mathbb{Z}$ and p if $\operatorname{im}\varphi \cong \mathbb{Z}_p$.*

(i) If char $F = p$ then F contains a subfield isomorphic to $\mathbb{F}_p$.

(ii) If char$F = 0$, then $\varphi : \mathbb{Z} \to F$ is injective. By universal property of fields of fractions, φ extends to $\mathbb{Q}$ with $\varphi : \mathbb{Q} \to F$. The extension is still injective (any morphism from a field to a nontrivial ring is injective). So F contains a subfield isomorphic to $\mathbb{Q}$.

*Every field F contains a copy of either of $\mathbb{F}_p$ or $\mathbb{Q}$. This is the **prime subfield** of F and is the smallest subfield of F.*

22.2 Field Extensions and Degree

Def. *A **Field Extension** is a pair of a field K and subfield F. Write $F \leq K$ or $K \mid F$ or $F - K$.*

Remark. *If K is a vector space over F it is a F-algebra.*

Def. *The **degree** of the extension is $[K : F] = \dim_F K$ (might be ∞).*

Remark. *A **ring extension** and the degree are defined similarly.*

Prop 22.1. *Let $F \leq L \leq K$ be field extensions. Then*

(a) If $[L : F] < \infty$ and $[K : L] < \infty$ then $[K : F] = [K : L][L : F] < \infty$.

(b) $[K : F] = \infty$ iff $[L : F] = \infty$ or $[K : L] = \infty$.

Proof.

(a) Let $\{\alpha_1, \ldots, \alpha_n\}$ be an F basis of L and $\{\beta_1, \ldots, \beta - m\}$ be an L-basis for K. Then note that $\{\alpha_i\beta_j\}$ is a basis for K over F.

(b) The forward comes from (a). The backward comes from constructing a basis of K.

□

Def. *Given a ring extension $R \leq S$ and $\alpha \in S$ then $R[\alpha]$ is the smallest subring of S with both R and α. This is true even if these are fields. But $F(\alpha)$ is the smallest subfield of $K \mid F$ that contains F and α. Note that these are not equal, in particular $F \leq F[\alpha] \leq F(\alpha) \leq K$ and $F(\alpha)$ is the Field of Fractions of $F[\alpha]$.*

Def. *K is a simple extension if $K = F(\alpha)$. α is the **primitive element** for the extension $K \mid F$ and K is obtained from F by **adjoining** α.*

Given $K \mid F$ and $\alpha \in K$, the universal property of polynomial algebra $F[x]$ yields F-algebra homomorphism $\varphi : F[x] \to K$ s.t. $\varphi(x) = \alpha$. We have $\varphi(a) = a$ for $a \in F$ and $\varphi(f(x)) = f(\alpha)$, so $\operatorname{im}\varphi = F[\alpha]$. Note that $\operatorname{im}\varphi$ is an integral domain (subring of K) so $\ker\varphi$ is a prime ideal in $F[x]$. Note that $\ker\varphi = \{0\}$ or $(p(x))$ since $F[x]$ is a PID. Therefore $F[x]/\ker\varphi \cong F[\alpha]$.

*If $\ker\varphi = \{0\}$ we say that α is **transcendental** over F. Equivalently there is no $g(x) \in F[x]$ s.t. $g \neq 0$ and $g(\alpha) = 0$. We have $F[x] = F(\alpha)$, which extends to $F(\alpha) = F(x)$, which are the **rational functions**.*

*If $\ker\varphi$ is nonzero, then α is **algebraic** over F. IE there is a nonzero $g(x)$ s.t. $g(\alpha) = 0$. So $\ker\varphi = (p(x))$ for some irreducible p (unique up to scaling) and $F[x]/(p(x)) \cong F[\alpha]$. Note that by maximality of $(p(\alpha))$ we have that $F[\alpha]$ is a field and so $F(\alpha) = F[\alpha] = \{f(\alpha : f(x) \in F[x])\}$. The unique **monic** irreducible $p(x)$ with $p(\alpha) = 0$ is the **minimum polynomial** of α over F, $m_{\alpha,F}(x)$ (or in some other contexts $irr(\alpha, F)(x)$). The degree of this is the **degree of** α **over** F, $\deg\alpha$.*

Prop 22.2. *Given $K \mid F$ let $\alpha \in K$ be algebraic over F. Then $\deg\alpha = [F(\alpha) : F]$.*

Proof. Claim that $\{1, \overline{x}, \ldots, \overline{x^{n-1}}\}$ is a basis for $F[x]/(p(x))$. □

Corrollary. *Let $K \mid F$ and $\alpha \in K$. α is algebraic over F iff $[F(\alpha) : F] < \infty$.*

Proof. Forward shown by above. Backward is shown that if transcendental then $F(\alpha) \cong F(x) \geq F[x]$ but this means that$F(\alpha) : F] \geq \dim_F F[x] = \infty$. □

22.3 Finite, Algebraic, and Finitely Generated Field Extensions

Def. *$K \mid F$ is finite if $[K : F] < \infty$. It is **algebraic** if every $\alpha \in K$ is algebraic over F. It is transcendental when it is not algebraic.*

Prop 22.3. *$K \mid F$ is finite implies that it is algebraic.*

Proof. Let $\alpha \in K$ and $F \leq F(\alpha) \leq K$. Then $[F(\alpha) : F] \leq [K : F] \leq \infty$ and as such α is algebraic over F for arbitrary α. □

Remark. *We note that* $F[\alpha_1, \dots, \alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n]$.

Def. *If there exists* $\alpha_i \in K$ *s.t.* $K = F(\alpha_1, \dots, \alpha_n)$, *we say that* $K \mid F$ *is finitely generated.*

23 Nov 21

23.1 More Field Extensions

Prop 23.1. *Let* $K \mid F$, $\alpha_1, \dots, \alpha_n \in K$ *s.t.* α_i *is algebraic over* $F(\alpha_1, \dots, \alpha_{i-1})$. *Then* $F(\alpha_1, \dots, \alpha_n) \mid F$ *is finite which implies it is algebraic and* $F(\alpha_1, \dots, \alpha_n) = F[\alpha_1, \dots, \alpha_n]$.

Remark. *If* α_i *algebraic over* F *for all* i, *then this is stronger than our prop.*

Proof. Induction on n. For $n = 0$ then we are done. Let $n \geq 1$. Let $L = F(\alpha_1, \dots, \alpha_{n-1})$. By induction hypothesis, $L \mid F$ finite and $L = F[\alpha_1, \dots, \alpha_{n-1}]$ where $F(\alpha_1, \dots, \alpha_n) = L(\alpha_n)$ where α_n algebraic over L which implies that $[L(\alpha_n) : L] < \infty$ and $L(\alpha_n) = L[\alpha_n]$. Hence $[L(\alpha_n) : F] = [L(\alpha_n) : L][L : F] < \infty$. Note that $F(\alpha_1, \dots, \alpha_n) = L(\alpha_n) = L[\alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n]$. $\square$

Corrollary. $K \mid F$ *finite iff* $K \mid F$ *algebraic and finitely generated.*

Proof. ($\Leftarrow$) is our proposition. ($\Rightarrow$) is because finite implies algebraic (last time). If $F = K$ then done. Let $\alpha \in K \setminus F$. If $K = F(\alpha)$ then done. If not then there exists a $\beta \in K \setminus F(\alpha)$ s.t. $F \subset F(\alpha) \subset F(\alpha, \beta) \subset \dots K$. The dimension (as vector spaces of F) at each stage is increasing by at least one and the dimension of K is finite, so this must eventually stop. $\square$

Def. *Given* $K \mid F$, *the* ***algebraic closure*** *of* F *in* K *is* $\Omega_K(F) = \{\alpha \in K : \alpha \text{ algebraic over } F\}$. *Note that* $F \leq \Omega_K(F) \leq K$.

Corrollary. $\Omega_k(F)$ *is a subfield of* K.

Proof. Let $\alpha, \beta \in K$ that are algebraic over F. We need that $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ if $\beta \neq 0$ are all algebraic over F. All these elements are in $F(\alpha, \beta) \subseteq K$. By the prop, $F(\alpha, \beta) \mid F$ algebraic. $\square$

Remark (Variants of UD of $F(x)$)**.** *Let* $\varphi : F \to R$ *be a ring homomorphism. Let* $\alpha \in R$. *Then there exists a unique ring homomorphism* $\varphi : F[x] \to R$ *extending* φ *and sending* $x \to \alpha$.

$$\begin{tikzcd} F[x] \arrow[r, dotted, "\varphi"] & R \\ F \arrow[u, hook] \arrow[ur, "\varphi"] & \end{tikzcd}$$

Our interpretation is that a field homomorphism $\varphi : F \to \tilde{F}$ extends uniquely to a ring homomorphism $\varphi : F[x] \to \tilde{F}[x]$ by

$$\begin{tikzcd} F[x] \arrow[r, dotted, "\varphi"] & \tilde{F}[x] \\ F \arrow[u, hook] \arrow[r, "\varphi"] & \tilde{F} \arrow[u, hook] \end{tikzcd}$$

By $\varphi(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0 + \varphi(a_1)x + \ldots \varphi(a_n)x^n$.

23.2 Root Adjunction

Prop 23.2. *F a field, $p(x) \in F[x]$ irreducible. Let $K = F[x]/(p(x))$ and $\alpha = \overline{x} \in K$. Then*

1. *K is a field and $F \hookrightarrow K$ and $p(\alpha) = 0$.*
2. *If K' is another field and $F \hookrightarrow K'$, $\alpha' \in K'$ with $p(\alpha') = 0$, then there exists a unique homomorphism of fields $\varphi : K \to K'$ s.t. $\varphi\mid_F = \mathrm{id}, \varphi(\alpha) = \alpha'$ and $F \hookrightarrow K, K'$ where $K \xrightarrow{\varphi} K'$.*

Proof. For 1, $p(x)$ is irreducible and is mapped to a PID so $(p(\alpha))$ is maximal which implies that K is a field. $F \hookrightarrow F[x] \twoheadrightarrow F[x]/(p(x)) = K$ so $F \hookrightarrow K$. $p(\alpha) = p(\overline{x}) = \overline{p(x)} = \overline{0}$.

For 2, given $F \hookrightarrow K'$, extend to $F[x] \to K'$ with $x \to \alpha'$. Note $\varphi(p(x)) = p(\alpha') = 0$. By UPQ, get $\varphi : K \to K'$.

$$\begin{tikzcd} F[x] \arrow[r, two heads] & F[x]/(p(x)) \arrow[r, "\varphi"] & K' \\ & F \arrow[ul, hook] \arrow[u, hook] \arrow[ur, hook] & \end{tikzcd}$$

□

Corrollary. *F field, $f(x) \in F[x]$ with $n = \deg(P) \geq 1$. Then there exists a field K and $F \hookrightarrow K$ and $\alpha \in K$ s.t. $f(\alpha) = 0$. Moreover, K can be chosen s.t. $[K : F] \leq n$.*

Proof. Apply proposition (1) toa ny irreducible factorization of $f(x)$. Then $[K : F] = \deg(p) \leq \deg(f) = n$. □

23.3 Splitting Fields

Def. *Let F be a field an $f(x) \in F[x]$. A **splitting field** over F is a field $K \geq F$ and containing elements $\alpha_1, \ldots, \alpha_n$ s.t.*

1. *$f(x) \sim (x - \alpha_1) \ldots (x - \alpha_n)$*
2. *$K = F(\alpha_1, \ldots, \alpha_n)$.*

Prop 23.3 (Existence of splitting fields)**.** *$f(x) \in F[x]$ where $\deg(f) = n$. There exists a splitting field K of $f(x)$ over F with $[K : F] \leq n!$.*

Proof. Use corollary: there exists a field $L \geq F$ and $\alpha_1 \in L$ s.t. $f(\alpha_1) = 0$ with $[L : F] \leq n$. Let $F_1 = F(\alpha_1) \leq L$. In $F_1[x]$ we have $f(x) = (x - \alpha_1)g(x)$ which implies that $\deg(g) = n - 1$. We now induct on $g(x)$. There exists a splitting field K of $g(x)$ over F_1 with $[K : F_1] \leq (n-1)!$ which implies that there exist $\alpha_2, \ldots, \alpha_n \in K$ s.t. $g(x) \sim (x - \alpha_2) \ldots (x - \alpha_n)$ and $K = F_1(\alpha_2, \ldots, \alpha_n$. Hence $[K : F] = [K : F_1][F_1 : F] \leq (n-1)!n = n!$. Note that $f(x) = (x - \alpha_1)g(x) \sim (x - \alpha_1) \ldots (x - \alpha_n)$ and $K = F_1(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$. $\square$

24 Nov 26

24.1 Splitting Fields cont

Lemma. *Let $f(x) \in F[x]$ and take K a splitting field of $f(x)$ over F. Let $\alpha \in K$ be a root of $f(x)$ and write $f(x) = (x - \alpha)f_1(x)$ with $f_1(x) \in K[x]$. Let $F_1 = F(\alpha)$. Then K is the splitting field of $f_1(x)$ over F_1.*

Proof. Note $f_1(x) \in F_1[x]$. We have $f(x) \sim (x - \alpha_1) \ldots (x - \alpha_n)$ in $K[x]$. and $K = F(\alpha_1, \ldots, \alpha_n)$ assume $\alpha = \alpha_1$ which implies that $f_1(x) \sim (x - \alpha_2) \ldots (x - \alpha_n)$ and $K = F_1(\alpha_2, \ldots, \alpha_n)$. $\square$

Prop 24.1 (Uniqueness of splitting fields)**.** *Let $\varphi : F \to \tilde{F}$ be a field isomorphism. let $f(x) \in F[x]$ and $\tilde{f}(x) = \varphi(f(x)) \in \tilde{F}[x]$. Let K be a splitting field of $f(x)$ over F and $\tilde{K}$ be a splitting field of $\tilde{f}(x)$ over $\tilde{F}$. Then φ can be extended to an isomorphism*

$$\begin{tikzcd} K \arrow[r, dotted] \arrow[d, dash] & \tilde{K}K \arrow[d, dash] \\ F \arrow[r, "\varphi"] & \tilde{F} \end{tikzcd}$$

Note that φ need not be unique.

Proof. Induction on $m = \deg(f(x))$. IF $n = 0$ then $K = F, \tilde{K} = \tilde{F}$ and we are done. Assume $n \geq 1$. Let $\alpha \in K$ be a root of $f(x)$. Let $F_1 = f(\alpha)$, $f_1(x) \in F_1[x]$ as in lemma. So K is a splitting field of $f_1(x)$ over F_1. Let $p(x) = m_\alpha, F(x) \in F[x]$ and $\tilde{p}(x) = \varphi(p(x)) \in \tilde{F}[x]$. We have that $f(\alpha) = 0 \implies p(x) \mid f(x)$ in $F[x]$. This implies that $\tilde{p}(x) \mid \tilde{f}(x)$ in $\tilde{F}[x]$ so there exists $\tilde{\alpha} \in \tilde{K}$ s.t. $\tilde{p}(\tilde{\alpha}) = 0$. Then $\tilde{p}(x) = m_{\tilde{\alpha},\tilde{F}}(x)$ Let $\tilde{F_1} = \tilde{F}(\tilde{\alpha})$. We know that $F_1 \cong F[x]/(p(x)) \xrightarrow{\varphi} F[x]/(\tilde{p}(x)) \cong \tilde{F_1}$. Let $\varphi_1 : F_1 \to \tilde{F_1}$ be the composite. $\varphi_1(\alpha) = tilde\alpha$. Consider $\tilde{f_1}(x) = \varphi 1(f_1(x)) \in \tilde{F_1}[x]$. We need to show that $\tilde{K}$ is a splitting field of $\tilde{f_1}(x)$ over $\tilde{F_1}$. Also follows from lemma because $\tilde{f}(x) = (x - \tilde{\alpha})\tilde{f_1}(x)$ where $f(x) = (x - \alpha)f_1(x)$. □

Corrollary. *Let F be a field and K and k' splitting fields for the same $f(x) \in F[x]$. Then there exists an isomorphism $\varphi : K \to K'$ s.t. $\varphi \mid_F = id$.*

Proof.
$$\begin{tikzcd} K \arrow[r, dotted, "\varphi"] & K' \\ F \arrow[u, hook] \arrow[r, "\text{id}"] & F \arrow[u, hook] \end{tikzcd}$$
□

24.2 Separability

Def. *$f(x) \in F[x]$ is **separable** if all its roots in some splitting field are distinct.*

Lemma. *Let $f(x) \in F[x]$ be separable and K some extension o fF. Then all roots of $f(x)$ that are in K are distinct.*

Proof. Let $\tilde{K}$ be a splitting field of $f(x)$ over K ie $f(x) \sim (x-\alpha_1)\dots(x-\alpha_n)$ in $\tilde{K}[x]$ and $\tilde{K} = K(\alpha_1, \dots, \alpha_n)$. Any root α in K must be one of the α_i's and $f(x) \sim (x - \alpha_1)\dots(x - \alpha_n)$ in $F(\alpha_1, \dots, \alpha_n)[x]$ implies that $F(\alpha_1, \dots, \alpha_n)$ is a splitting field of $f(x)$ over F which implies the α_i's are distinct. □

Def. *Given $f(x) \in F[x]$ its **derivative** defined $f(x) = \sum_{i=0}^n a_i x_i \to f'(x) = \sum_{i=1}^m i a_i x^{i-1}$.*

Remark. *The properties hold ie $(f+g)' = f'+g', (f \cdot g)' = f'g+fg', f(g(x))' = f'(g(x)) \cdot g'(x)$.*

Remark. *If $i \in \mathbb{N}$ and $a \in F$, then $ia = a + a + \dots + a$. In fact it lies in the prime field of F in the $\mathbb{F}_p$ on $\mathbb{Q}$. if it is $\mathbb{F}$ then $i1 = 0 \iff p \mid i$.*

Prop 24.2. *$f(x) \in F[x]$, K a splitting field over F. The following are equivalent*

(i) $f(x)$ *is separable.*

(ii) $f(x)$ *and* $f'(x)$ *have no common roots in* K

(iii) $\gcd(f(x), f'(x)) \sim 1$ *take in* $F[x]$.

Corrollary. *Let $p(x) \in F[x]$ be irred. Then $p(x)$ is separable iff $p'(x) \neq 0$.*

Proof. ($\Rightarrow$) If $p'(x) = 0$ then $p(x)$ and $p'(x)$ have common roots (all roots of $p(x)$) which is a contradiction. ($\Leftarrow$) suppose $p(x)$ not separable. By three this implies that $d(x) = \gcd(f(x), f'(x)) \not\sim 1$ which implies that $d(x) \mid p(x) \implies d(x) \sim p(x)$ and $d(x) \mid p'(x)$ but this implies that $p(x) \mid p'(x)$ which implies that $p'(x) = 0$, a contradiction. $\square$

Corrollary. *Suppose that* $\operatorname{char} F = 0$. *Then Any irreducible polynomial is separable.*

Ex. *$F = \mathbb{F}_p(y)$ rational functions. Let $f(x) = x^p - y \in F[x]$. Know that $f(x)$ is irreducible in $F[x]$ by Gauss Lemma. This is not separable because $f'(x) = px^{p-1} = 0$.*

Let K be a splitting field of $f(x)$ over F and let $\alpha \in K$ be a root of $f(x)$. This implies that $0 = f(\alpha) = \alpha^p - y$ which implies that $\alpha^p = y$ then $f(x) = x^p - \alpha^p = (x - \alpha)^p$.

25 Dec 3

25.1 Finalizing Separability

Def. *Given $k \mid F$, $\alpha \in K$ is **separable over** F if it is algebraic and $m_{\alpha,F}(x)$ is separable.*

Remark. *If char $F = 0$ or $|F| < \infty$, every algebraic element is separable.*

Theorem 25.1 (Primitive Element Theorem)**.** *Let $K = F(\alpha_1, \dots, \alpha_n)$ with all α_i algebraic over F and $\alpha_2, \dots, \alpha_n$ are separable over F. Then there exists $\gamma \in K$ s.t. $K = F(\gamma)$.*

Proof. Skipped for time but read it yourself. $\square$

25.2 Algebraic Independence

Def. *Given $K \mid F$ elements $\alpha_1, \dots \alpha_n \in K$ is **algebraically independent** (a. i.) if there doesn't exist an $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n] \setminus \{0\}$ s.t. $f(\alpha_1, \dots, \alpha_n) = 0$.*

Let $\varphi : F[x_1, \dots, x_n] \to K$ be an evaluation at $\alpha_1, \dots, \alpha_n$. Then $\alpha_1, \dots, \alpha_n$ are aa.i. iff φ is injective. So φ extends to $\varphi : F(x_1, \dots, x_n) \to K$ and this is still injective. In particular, $[K : F] = \infty$.

Prop 25.1. *$K \mid F$, $\alpha_1, \dots, \alpha_n \in K$. The following are equivalent*

(i) *$\alpha_1, \dots, \alpha_n$ are a.i. over F.*

(ii) *Each α_i is transcendental over $F(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_n)$ where $\widehat{\alpha_i}$ is α_i omitted.*

(iii) *Each α_i is transcendental over $F(\alpha_1, \dots, \alpha_{i-1})$.*

Proof. $1 \implies 2$ suppose α_i is algebraic over $F(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_n)$ for some i. This implies that there exists a nontrivial polynomial $\sum a_j \alpha_i^j = 0$ on the elt $a_j \in F[\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_n]$. But this is a nontrivial polynomial in $\alpha_1, \dots, \alpha_n$.

$2 \implies 3$ because $F(\alpha_1, \dots, \alpha_{i-1}) \leq F(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_n)$.

$3 \implies 1$. We dot it for $n = 2$. Given α trans over F, β trans over $F(\alpha)$. We want $\{\alpha, \beta\}$ is a.i. over F. Let $f(x, y) \in F[x, y] \setminus \{0\}$. Write $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$ with some $a_{nm} \neq 0$. This implies $f(x, y) = \sum_j \left(\sum_i a_{ij}\right) x^i y^j = \sum_j a_j(x) y^j$. $a_m(x) = \sum_i a_{i,m} x^j \neq 0$ because $a_{nm} \neq 0$. α is trans in F implies that $a_m(\alpha) \neq 0$ which implies $f(\alpha, y) = \sum_j \alpha_j(\alpha) y^j \in F(\alpha)[u] \setminus \{0\}$. β trans in $F(\alpha)$ implies that $f(\alpha, \beta) \neq 0$. □

Def. *$K \mid F$ is **purely transcendental** if $\exists$ $\alpha_1, \dots, \alpha_n$ a.i. over F s.t. $K = F(\alpha_1, \dots, \alpha_n)$. In particular each α_i is trans over F.*

Def. *Given $K \mid F$, a set of elements $\alpha_1, \dots, \alpha_n \in K$ is a **finite transcendence basis** for $K \mid F$ if*

1. *$\alpha_1, \dots, \alpha_n$ are a.i. over F*
2. *$K \mid F(\alpha_1, \dots, \alpha_n)$ is algebraic.*

Prop 25.2. *Let $K \mid F$ be a f.g. extension. $K = F(S)$ for some finite set $S \subseteq K$. Then S contains a transcendental basis for $K \mid F$.*

Proof. Build $\alpha_1, \ldots, \alpha_d$ by picking elements of S one at a time, so that each step α_i is trans over the preceding ones. Because S is finite this process stops at α_d. This implies that there doesn't exist an element in S trans over $F(\alpha_1, \ldots, \alpha_d)$ which implies that $K = F(S) \mid F(\alpha_1, \ldots, \alpha_d)$ is algebraic.

So α_1 is trans over F, and in particular α_i is trans over $F(\alpha_1, \ldots, \alpha_{i-1})$ for $i \in [d]$. By our previous prop part 3, $\{\alpha_1, \ldots, \alpha_d\}$ is a.i. over F. $\square$

Def. *Let $K \mid F$ be a finitely generated extension. The **transcendence degree** of $K \mid F$, $tr_F K$ is the site of transcendence basis. Next time we will show that this size is well defined ie $tr_F K = 0 \iff K \mid F$ algebraically.*

Ex. *$K = F(x, y, z)$ rational functions on x, y, z. We claim that $\{x, y, z\}$ is a.i. over F which implies $F[x, y, z] \to K$ is just the inclusion $x, y, z \to x, y, z$. It is a fact that $\{xy, xz, yz\}$ is also a.i.The algebraic dependents among $\{x, y, z, xy, xz, yz, xyz\}$ are described by a simplex where $x - xy - y$ on the sides and xyz is in the middle and is connected to all others. Note that $f(r, s, t) = rs - t$ vanishes on $\{x, y, xy\}$.*

Remark. *Compare with linear dependence. Let $\{x, y, z\}$ be a basis for a 3-dimensional F-vector space. $\{x, y, z, x+y, x+z, y+z, x+y+z\}$. The linear dependencies are captured by the same diagram but when char $F = 2$ then it forms the Fano Plane. Note that any two are li and when 3 elements are ld we put them in a line.*

Ex. *$\mathbb{R}[S^1] = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$. We claim that $x^2 + y^2 - 1$ is irreducible in $\mathbb{R}[x, y] = R[x]$. $x^2 + y^2 - 1 \in R[x] \subset F[x]$ where $R = \mathbb{R}[y], F = \mathbb{R}(y)$. This polynomial is primitive since it is $x^2 + (y^2 - 1)$ as $\gcd(1, y^2 - 1) = 1$. It is irreducible in $F[x]$, since if not there is a root $\alpha \in F$ of $x^2 + y^2 - 1$. But by the rational root theorem there is a root $\alpha \in R$. We have that $\alpha^2 + y^2 - 1$ but if $\alpha = \sum_i a_i y^i$ then $(\sum a_i y^i)^2 + y^2 - 1$ but we have that $a_0^2 - 1 = 0, a_1^2 + 1 = 0$ but this is impossible, so this polynomial is irreducible.*

$\mathbb{R}[s^1]$ is an integral domain. Let $R(s^1)$ be its field of fractions and $\alpha = \overline{x}$, $\beta = \overline{y} \in \mathbb{R}[S^1] \subseteq \mathbb{R}(S^1)$ which implies that $\mathbb{R}[S^1] = \mathbb{R}[\alpha, \beta], \mathbb{R}(S^1) = \mathbb{R}(\alpha, \beta)$. Clearly α is trans over $\mathbb{R}$. If not there exists an $f(x) \in \mathbb{R}[x] \setminus \{0\}$ s.t. $f(\alpha) = 0$ which implies that $\overline{f(x)} = \overline{0}$ in $\mathbb{R}[xy]/(x^2 + y^2 - 1)$ which implies that $x^2 + y^2 - 1 \mid f(x) \implies f(x) = 0$ (otherwise infinite number of roots).

We see that β is algebraic over $R(\alpha)$ because $\alpha^2 + \beta^2 - 1 = 0$ which implies $\{\alpha\}$ is trans for $\mathbb{R}(S^1) \mid \mathbb{R}$ which implies that $tr_{\mathbb{R}} \mathbb{R}(S^1) = 1$. Note that this has a lot to do with algebraic geometry (it is the dimension of the variety *and is based off of Noether's normalization theorem and that fact that* $\mathbb{R}[S^1]$ *is an integral domain).*

26 Dec 5

27 Dec 10

27.1 Artin-Tate

Remark. *Recall that the original formulation of Artin-Tate. If* $R \leq S \leq T$ *are Noetherian rings and* T *is finitely generated as an* S*-module and* S *is finitely generated as an* R*-algebra, then* T *is finitely generated as an* R*-algebra.*

Remark. *Let* $F \leq K$ *be fields. There are* 3 *types of finite generation for* K *over* F*. (1) If* K *is finitely generates as an* F*-module iff* $\dim_F K < \infty$ *iff* $K \mid F$ *extension is finite. (2)* K *is finitely generated as an* F*-algebra with* $K = F[\alpha_1, \ldots, \alpha_n]$ *for some* $\alpha_i \in K$*. (3)* K *is finitely generated as a field extension of* F *ie* $K = F(\alpha_1, \ldots, \alpha_n)$ *for some* $\alpha_i \in K$*. Clearly* $(1) \Rightarrow (2) \Rightarrow (3)$*. But* $(3) \not\Rightarrow (2)$ *but* $(2) \Rightarrow (1)$*.*

Lemma. *If* $d \geq 1$ *the field of rational functions* $F(x_1, \ldots, x_d)$ *is not finitely generated as an* F*-algebra.*

Proof. Suppose it is: $F(x_1, \ldots, x_d) = F[\alpha_1, \ldots, \alpha_n]$, $\alpha_i \in F(x_1, \ldots, x_d)$ wher e$\alpha_i \in F(x_1, \ldots, x_d0$. Write $\alpha_i = f_i/g_i$ with $f_i, g_i \in F[x_1, \ldots, x_d]$. If all g_i are units this implies $\alpha_i \in F[x_1, \ldots, x_d]$ which implies that $F(x_1, \ldots, x_d) = F[x_1, \ldots, x_d]$ which is not a field for $d \geq 1$. At least the g_i is not constant which implies that $1 + g_1 \ldots g_n$ is not constant. So it has an irreducible factors $p \in F[x_1, \ldots, x_d]$ and as such $\frac{1}{p} \in F(x_1, \ldots, x_d) = F[\alpha_1, \ldots, \alpha_n]$. Cleaning denominators, we have that $\frac{g_1 - g_n)^N}{p} \in F[x_1, \ldots, x_d]$ which implies that $p \mid (g_1 \ldots g_n)^N$ in $F[x_1, \ldots, x_d]$ which implies that $p \mid g_j$ for some j. But $p \mid 1 + \ldots g_1 \ldots g_n$ which implies $p \mid 1$, which is a contradiction. $\square$

Remark. *This is similar to the proof that there are infinite number of primes.*

Theorem 27.1 (Zariski)**.** *Let* $K \mid F$ *be a field extension. if* K *is finitely generated as* F*-algebra this implies that* $\dim_F K < \infty$*.*

Proof. Recall that $(2) \Rightarrow (3)$. $K \mid F$ is finitely generated as a field extension. We need that $K \mid F$ algebraically (and finitely generated implies finite). Recall that $K \mid F$ has a finite trans basis $\alpha_1, \ldots, \alpha_d$. We need to $d = 0$.

By hypothesis, $K \mid F$ is a finitely generated as an algebra. K is finitely generated as an $F(\alpha_1, \ldots, \alpha_d)$-module because $K \mid F(\alpha_1, \ldots, \alpha_d)$ is finitely generated and algebraic. By Artin-Tate: $F(\alpha_1, \ldots, \alpha_d)$ is finitely generated as an F-module, which implies that $F(\alpha_1, \ldots, \alpha_d) \mid F$ is finite, which implies that this is algebraic, so $d = 0$. $\square$

27.2 Some first notions of Algebraic Geometry

Corrollary (Weak Nullstellensatz)**.** *Let F be a field, R a nontrivial commutative finitely generated F-algebra. Let M be a maximal ideal of R and $K = R/M$. Then K is a finite field extension of F.*

Proof. Consider $F \hookrightarrow R \twoheadrightarrow R/M = K$ where we map $F \to R$ by $\lambda \to \lambda \cdot 1$.. This is injective since F is a field. R finitely generated as an F-algebra implies that K is finitely generated as an F-algebra. By Zariski, $\dim_F K < \infty$. $\square$

Def. *The **maximal spectrum** of a commutative ring R is $Spec_M(R) = \{M : M \text{ max ideal of } R\}$. Given F-algebras R, S, let $Alg_F(R, s) = \{\varphi : R \to S : \varphi \text{ a morphism of } F\text{-algebras}\}$.*

Corrollary. *Let F be an **algebraically closed** field F. Let R be a finitely generated F-algebra. Then $Alg_F(R, F) \to Spec_M(R)$ from $\varphi \to \ker\varphi$ is a bijection.*

Proof. We show that for $\varphi : \mathrm{Alg}_F(R, F) \implies \varphi \mid_F = \mathrm{id}_F \implies \varphi$ is onto $\implies R/\ker\varphi \cong \operatorname{im}\varphi = F$ field which implies $\ker\varphi$ is maximal. So this map is well defined.

This map is injective because because if $\ker\varphi = \ker\psi$ then $a - \varphi(a) \cdot 1 \in \ker\varphi = \ker\psi \implies \psi(a) = \varphi(a)$.

This map is surjective. Take $M \in \mathrm{Spec}_M(R)$. Consider that $\varphi : R \twoheadrightarrow R/M = K = F$. $K \mid F$ is finite which implies that $K = F$ since F is algebraically closed. φ is an F-algebra homomorphism with $\ker\varphi = M$. $\square$

Def. *Given $S \subseteq F[x_1, \ldots, x_n]$. let $\mathcal{Z}(S) = \{a \in F^n : f(a) = 0 \forall f \in S\}$. This is the **zero set/locus** of S.*

Let I be an ideal of $F[x_1, \ldots, x_n]$ and $R = F[x_1, \ldots, x_n]/I$. Then

$$\begin{tikzcd} F[x_1, \ldots, x_n] \arrow[r, "\varphi_a"] \arrow[d, two heads] & F \\ R \arrow[ur, dotted] & \end{tikzcd}$$

Given $a \in F^n$, let $\varphi_a : F[x_1, \dots, x_n] \to F$ be evaluated at $a : \varphi_a(f) = f(a)$. φ_a factors through R iff $\varphi_a(f) = 0 \forall f \in I$ iff $f(a) = 0 \forall f \in I$ iff $a \in \mathcal{Z}(I)$. Conclusion: there is a bijection between $\mathcal{Z}(I) \to Alg_F(R, F)$ by $a \to \varphi_a$.

Corrollary. *Let F be algebraically closed. Let I be an ideal in $F[x_1, \dots, x_n]$, $R = F[x_1, \dots, x_n]/I$. There is a bijection $\mathcal{Z}(I) \to Spec_M(R)$ by $a \to \ker \varphi_a$.*

Def. *Given $A \subseteq F^n$, let $\mathcal{I}(A) = \{f \in F[x_1, \dots, x_n] : f(a) = 0 \ \forall a \in A\}$. This is the **vanishing set** of A.*

Remark. *$\{$subsets of $F^n\}$ and $\{$subsets of $F[x_1, \dots, x_n]\}$ are mapped toe ach other by $\mathcal{I}$ and $\mathcal{Z}$ They are partially ordered by inclusion.*

Prop 27.1.

(1) $\mathcal{I}$ and $\mathcal{Z}$ are order-reversing.

(2) $A \subseteq \mathcal{Z}\mathcal{I}(A)$ for all $A \subseteq F^n$. Similarly $S \subseteq \mathcal{I}\mathcal{Z}(S)$ for all $S \subseteq F[x_1, \dots, x_n]$. So $\mathcal{I}, \mathcal{Z}$ is a Galois Connection.

(3) $\mathcal{I}\mathcal{Z}\mathcal{I} = \mathcal{I}$ and $\mathcal{Z}\mathcal{I}\mathcal{Z} = \mathcal{Z}$.

(4) $\mathcal{Z}$ and $\mathcal{I}$ induce inverse bijections.

Def. *A subset $A \subseteq F^n$ is **algebraic** if it is in $\operatorname{im} \mathcal{Z}$.*

Def. *Let R be a commutative ring, I and ideal. The **radical of** I is $\sqrt{I} = \{a \in R : a^n \in I, \text{ for some } n \in \mathbb{N}\}$. This is also an ideal.*

Theorem 27.2 (Strong Nullstellensatz)**.** *F algebraically closed and I is an ideal of $F[x_1, \dots, x_n]$. Then $\mathcal{I}\mathcal{Z}(I) = \sqrt{I}$.*

Remark. *Nullstellensatz translates to theorem of the locus of the zeros.*

Corrollary. *The image of $\mathcal{I}$ is the set of **radical ideals**.*

Proof. $R = F[x_1, \dots, x_n]/I$. Given $a \in F^n$

$$\begin{tikzcd} F[x_1, \dots, x_n] \arrow[r, "f_a"] \arrow[d, two heads] & I \\ R \arrow[ur, "\widehat{\varphi_a}"] & \end{tikzcd}$$

$f \in \mathcal{I}\mathcal{Z}(I) \iff f(a) = 0, \forall a \in \mathcal{Z}(I) \iff \varphi_a(f) = 0, \forall a \in \mathcal{Z}(I) \iff \overline{f} \in \ker \widehat{\varphi_a} \forall a \in \mathcal{Z}(I) \iff \overline{f}$ is in all maximal ideals of R. But this occurs iff $\overline{f}$ is nilpotent (ie there exists $n \in \mathbb{N}$ s.t. $\overline{f}^n = \overline{0}$) iff there exists $n \in \mathbb{N}$ s.t. $f^n \in I$ iff $f \in \sqrt{I}$, as desired. □