Note that we can also show the converse of Hilbert's basis theorem. In other words, A is a Noetherian ring if $A[x]$ is Noetherian.

Proof:
Suppose A isn't a Noetherian ring. Then there exists a sequence $\{\mathfrak{a}_n\}_{n\in\mathbb{N}}$ of ideals in A such that $\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \cdots$. In turn, $\{\mathfrak{a}_n[x]\}_{n\in\mathbb{N}}$ is also a sequence of ideals in $A[x]$ such that $\mathfrak{a}_1[x] \subsetneqq \mathfrak{a}_2[x] \subsetneqq \cdots$. This proves that $A[x]$ isn't a Noetherian ring. ■

Also note that if A is Noetherian and $\mathfrak{a} \lhd A$, then we have that $A/\mathfrak{a}$ is Noetherian.

Proof:
By the correspondance theorem we know that any ideal of $A/\mathfrak{a}$ is of the form $\mathfrak{b}/\mathfrak{a}$ where $\mathfrak{b} \lhd A$ with $\mathfrak{a} \subseteq \mathfrak{b}$. Since A is Noetherian, we know that $\mathfrak{b}$ is finitely generated. In turn, we also know that $\mathfrak{b}/\mathfrak{a}$ is finitely generated. ■

12/10/2025

Today I'm preparing for the math 200a final and also taking some miscellaneous notes on topics that came up while I was doing practice problems.

Recall how if n is an integer and p is a prime then we defined:
$$\nu_p(n) = \max\{k \in \mathbb{Z}_{\geq 0} : p^k \mid n\}.$$

We can extend ν_p to being defined on $\mathbb{Q}$ as follows. Given any rational number ${}^m/_n \neq 0$ we define $\nu_p({}^m/_n) = \nu_p(m) - \nu_p(n)$.

To prove this is well-defined, suppose $\frac{m_1}{n_1} = \frac{m_2}{n_2}$. Then after canceling common prime factors of m_i and n_i, we can find pairs of integers m_i', n_i' such that for each i:
$$\frac{m_i'}{n_i'} = \frac{m_i}{n_i},\ \gcd(m_i, n_i) = 1, \text{ and } \nu_p(m_i') - \nu_p(n_i') = \nu_p(m_i) - \nu_p(n_i)$$

But now it is easy to check that $m_1' = m_2'$ and $n_1' = n_2'$. After all, we know that $\frac{m_1'}{n_1'} = \frac{m_2'}{n_2'} \iff m_1'n_2' = m_2'n_1'$. Then by comparing the prime factorings of both sides of the latter equation and noting that m_i' and n_i' are coprime for each i, we can show that $m_1' = \pm m_2'$ and $n_1' = \pm n_2'$. Yet the sign of m_1' doesn't effect $\nu_p(m_1')$. ■

Note that since $\nu_p(n_1 n_2) = \nu_p(n_1)\nu_p(n_2)$ when $n_1, n_2 \in \mathbb{Z}$, we can easily show that $\nu_p(rs) = \nu_p(r) + \nu_p(s)$ for all $r, s \in \mathbb{Q} - \{0\}$. We can also easily see that $\nu_p(r^{-1}) = -\nu_p(r)$ for all $r \in \mathbb{Q}$.

Problem 2 From Fall 2024 Midterm: Suppose G is a finite group, p is a prime integer, and H, K are 2 subgroups of G such that $G = HK$.

(a) Prove that there exists $P \in \mathrm{Syl}_p(G)$ such that $P \cap H \in \mathrm{Syl}_p(H)$ and $P \cap K \in \mathrm{Syl}_p(K)$.

Pick $Q_H \in \mathrm{Syl}_p(H)$ and $Q_k \in \mathrm{Syl}_p(K)$. By Sylow's second theorem, there exists $P_1, P_2 \in \mathrm{Syl}_p(G)$ such that $Q_H \subseteq P_1$ and $Q_k \subseteq P_2$.

We claim that $Q_H = P_1 \cap H$.

To see why, note that $P_1 \cap H$ must be a p-group containing Q_H. Furthermore, if $P_1 \cap H$ properly contained Q_H then that would contradict that Q_H is a Sylow p-subgroup.

Similarly, we have that $Q_K = P_2 \cap K$.

But now note by Sylow's second theorem plus the fact $G = HK$ that there must exist $h \in H$ and $k \in K$ such that $P_1 = hkP_2k^{-1}h^{-1}$. Hence, we may let $P := h^{-1}P_1h = kP_2k^{-1}$ and know that $P \in \mathrm{Syl}_p(G)$.

Finally, $P \cap H = h^{-1}(P_1 \cap H)h = h^{-1}Q_Hh \in \mathrm{Syl}_p(H)$ and

$$P \cap K = k(P_2 \cap K)k^{-1} = kQ_Kk^{-1} \in \mathrm{Syl}_p(K).$$

By the way I got the final three sentences of this proof from Hagan.

(b) Suppose $P \in \mathrm{Syl}_p(G)$, $P_H := P \cap H \in \mathrm{Syl}_p(H)$, and $P_K := P \cap K \in \mathrm{Syl}_p(K)$. Then prove that $P = P_HP_K$.

To start off, we know that $|P_H| = p^{r_1}$, $|P_K| = p^{r_2}$, and $|P_H \cap P_K| = p^{r_3}$ where $r_3 \leq \min(r_1, r_2)$. It follows that $|P_HP_K| = |P_H||P_K|/|P_H \cap P_K| = p^\ell$ where $\ell = r_1 + r_2 - r_3 \geq 0$. Also note that $P_H \subseteq P$ and $P_K \subseteq P$ implies that $P_HP_K \subseteq P$. It follows that $p^\ell \leq |P| = p^{\nu_p(|G|)}$. Hence, we can conclude that $\ell \leq \nu_p(|G|)$. And from there it is clear that:

$$0 \leq \nu_p(\tfrac{|G|}{|P_HP_K|})$$

At the same time, note that:

$$\begin{aligned}\nu_p(\tfrac{|G|}{|P_HP_K|}) &= \nu_p(\tfrac{|H|}{|P_H|} \cdot \tfrac{|K|}{|P_K|} \cdot \tfrac{|P_H \cap P_K|}{H \cap K}) \\ &= \nu_p(\tfrac{|H|}{|P_H|}) + \nu_p(\tfrac{|K|}{|P_K|}) + \nu_p(\tfrac{|P_H \cap P_K|}{H \cap K}) = 0 + \nu_p(\tfrac{|P_H \cap P_K|}{H \cap K})\end{aligned}$$

Additionally, note that $P_H \cap P_K = (P \cap H) \cap (P \cap K) = P \cap (H \cap K)$. Hence, it follows that $P_H \cap P_K$ is p-subgroup of $H \cap K$ and therefore $\nu_p(\frac{|P_H \cap P_K|}{H \cap K}) \leq 0$.

With that we know that $\nu_p(\frac{|G|}{|P_HP_K|}) = 0$. Yet, we also know that $\nu_p(\frac{|G|}{|P|}) = 0$. It follows that $\nu_p(\frac{|P|}{|P_HP_K|}) = 0$, and this proves that $|P| = |P_HP_K|$. By invoking one last time that $P_HP_K \subseteq P$ we now know that $P = P_HP_K$. ■

Problem 5(b) from a past final: Suppose A is a (commutative unital) Noetherian ring and $\phi : A \to A$ is a surjective ring homomorphism. Then ϕ is an isomorphism.

Proof:

We need to show ϕ is injective, and to do that it suffices to show $\ker(\phi) = \{0\}$. Luckily note that $\ker(\phi^n) \subseteq \ker(\phi^{n+1})$ for all integers $n \geq 0$ (where we consider ϕ^0 to be the identity map). Thus since A is Noetherian, there must exist some smallest nonnegative integer N such that $\ker(\phi^{N+j}) = \ker(\phi^N)$ for all $j \in \mathbb{N}$.

Suppose $N > 0$. Then we can find $a \in A$ such that $\phi^{N-1}(a) = b \neq 0$ and $\phi(b) = \phi^N(a) = 0$. Yet also note that because ϕ is surjective, we can find $c \in A$ such that $\phi(c) = a$. In turn, we have that $\phi^N(c) = \phi^{N-1}(\phi(a)) = b \neq 0$ but $\phi^{N+1}(c) = \phi(\phi^N(c)) = \phi(b) = 0$. This contradicts that $\ker(\phi^{N+1}) = \ker(\phi^N)$. Hence, we conclude that we can't have that $N > 0$.

But now in particular we must have that $\{0\} = \ker(\phi^0) = \ker(\phi^1)$. ■

Another miscellaneous note I want to make is that if A, A' are both unital rings and $\phi : A \to A'$ is a ring homomorphism such that $1_{A'} \in \operatorname{im}(\phi)$ then we must have that $\phi(1_A) = 1_{A'}$.

After all, suppose $\phi(b) = 1_{A'}$ where b is any element in A. Then:

$$\phi(1_A) = \phi(1_A)1_{A'} = \phi(1_A)\phi(b) = \phi(1_A b) = \phi(b) = 1_{A'}.$$

Here's some homework problems from the past that I never finished.

Set 6 Problem 6: Suppose G is a group. For all $x, y \in G$, let $[x, y] := xyx^{-1}y^{-1}$ and ${}^x y := xyx^{-1}$. Then Hall's equation asserts that:

$$[[x, y], {}^y z][[y, z], {}^z x][[z, x], {}^x y] = 1.$$

To prove this, first note that:

$$\begin{aligned}[[a, b], {}^b c] &= (aba^{-1}b^{-1})(bcb^{-1})(bab^{-1}a^{-1})(bc^{-1}b^{-1}) \\ &= (aba^{-1})c(ab^{-1}a^{-1})(bc^{-1}b^{-1}) = {}^a b \cdot c \cdot {}^a(b^{-1}) \cdot {}^b(c^{-1})\end{aligned}$$

Also note that ${}^b(a^{-1}) \cdot {}^b a = bab^{-1} \cdot ba^{-1}b^{-1} = 1$. Therefore:

$$\begin{aligned}&[[x, y], {}^y z][[y, z], {}^z x][[z, x], {}^x y] \\ &= ({}^x y \cdot z \cdot {}^x(y^{-1}) \cdot {}^y(z^{-1}))({}^y z \cdot x \cdot {}^y(z^{-1}) \cdot {}^z(x^{-1}))({}^z x \cdot y \cdot {}^z(x^{-1}) \cdot {}^x(y^{-1})) \\ &= ({}^x y \cdot z \cdot {}^x(y^{-1}))(x \cdot {}^y(z^{-1}))(y \cdot {}^z(x^{-1}) \cdot {}^x(y^{-1})) \\ &= (xyx^{-1}zxy^{-1}x^{-1})(xyz^{-1}y^{-1})(yzx^{-1}z^{-1}xy^{-1}x^{-1}) \\ &= (xyx^{-1}zxy^{-1})(yz^{-1})(zx^{-1}z^{-1}xy^{-1}x^{-1}) \\ &= (xyx^{-1}zx)(x^{-1}z^{-1}xy^{-1}x^{-1}) = 1\end{aligned}$$

Next consider the lower central series $\gamma_1(G) = G$ and $\gamma_{i+1}(G) = [G, \gamma_i(G)]$ for all i.

Note that $[H_1, H_2] = [H_2, H_1]$ for any subgroups $H_1, H_2 < G$ since $([h_1, h_2])^{-1} = [h_2, h_1]$. So this definition is equivalent to the one in class.

(a) Suppose $H, K, L \lhd G$ and prove that $[[H, K], L] < [[K, L], H][[L, H], K]$.

To start off, as $H, K, L \lhd G$ we know that $[H, K]$, $[K, L]$, and $[L, H]$ are normal subgroups of G. In turn, we also know that $[[H, K], L]$, $[[K, L], H]$, and $[[L, H], K]$ are normal subgroups of G. And finally, this tells us that $[[K, L], H][[L, H], K]$ is a normal subgroup of G.

(See the lemma at the bottom of *page 378*. Also, I think I forgot to ever prove that if $N_1 \lhd G$ and $N_2 \lhd G$ then $N_1 N_2 \lhd G$. Fortunately, the proof is incredibly simple. $xN_1N_2x^{-1} = xN_1x^{-1}xN_2x = N_1N_2$ for all $x \in G$.)

Consider $\overline{G} \coloneqq \frac{G}{[[K,L],H][[L,H],K]}$. Then if $\pi : G \to \overline{G}$ is the natural projection homomorphism, let $\overline{H} = \pi(H)$, $\overline{K} = \pi(K)$, and $\overline{L} = \pi(L)$.

We claim for all $\overline{h} \in \overline{H}$, $\overline{k} \in \overline{K}$, and $\overline{l} \in \overline{L}$ that $[\overline{h}, \overline{k}]$ and $\overline{l}$ commute (where $\overline{x} = \pi(x) = x[[K,L],H][[L,H],K]$).

Note that $[[k,l],{}^{l}h][[l,h],{}^{h}k] \in [[K,L],H][[L,H],K]$ whenever $h \in H$, $k \in K$, and $l \in L$. This is because H and K are normal subgroups.

In turn, we can apply Hall's equation from the last page to get that:

$$\overline{[[h,k],{}^{k}l]} = \overline{[[h,k],{}^{k}l][[k,l],{}^{l}h][[l,h],{}^{h}k]} = \overline{1}$$

Therefore, we have that $[\overline{h}, \overline{k}]$ and $\overline{{}^{k}l}$ commute.

Finally, note that because L is a normal subgroup we know that conjugation by k is an automorphism on L. Hence, for any $l_1 \in L$ there exists $l_0 \in L$ with $kl_0k^{-1} = l$. Hence, substituting in l_0 for l in the above reasoning we've shown that $[\overline{h}, \overline{k}]$ and $\overline{l}$ commute for all $\overline{h} \in \overline{H}$, $\overline{k} \in \overline{K}$, and $\overline{l} \in \overline{L}$.

Going a step further, we claim that any element in $[\overline{H}, \overline{K}]$ commutes with any $\overline{l}$ in $\overline{L}$.

Suppose $x_1, \ldots, x_n$ are all commutators of $\overline{H}$ and $\overline{K}$. Then since each x_i individually commutes with $\overline{l}$, it's clear that:

$$x_1 \cdots x_{n-1} x_n \overline{l} = x_1 \cdots x_{n-1} \overline{l} x_n = \cdots = \overline{l} x_1 \cdots x_n$$

But now we've shown that $[[\overline{H}, \overline{K}], \overline{L}] = \{1\}$. And since surjective group homomorphisms pass in and out of the brackets in commutator subgroups, we know that $[[\overline{H}, \overline{K}], \overline{L}] = \pi([[H,K],L])$. Hence, $\overline{x} = \overline{1}$ in $\overline{G}$ for all $x \in [[H,K],L]$. And this proves that $[[H,K],L] < [[K,L],H][[L,H],K]$.

(b) Prove for every positive integers m and n that $[\gamma_m(G), \gamma_n(G)] \subseteq \gamma_{m+n}(G)$.

We shall proceed by induction on m.

Note by definition that $[\gamma_1(G), \gamma_n(G)] = [G, \gamma_n(G)] = \gamma_{n+1}(G)$. Thus our base case of $m = 1$ holds trivially.

Next, suppose $m > 1$ and that $[\gamma_k(G), \gamma_n(G)] \subseteq \gamma_{k+n}(G)$ for all $n \in \mathbb{N}$ and $k < m$. Then by part (a) we have for any $n \in \mathbb{N}$ that:

$$\begin{aligned}[\gamma_m(G), \gamma_n(G)] = [[G, \gamma_{m-1}(G)], \gamma_n(G)] &\subseteq [[\gamma_{m-1}(G), \gamma_n(G)], G][[\gamma_n(G), G], \gamma_{m-1}(G)] \\ &\subseteq [\gamma_{m+n-1}(G), G][\gamma_{n+1}(G), \gamma_{m-1}(G)] \\ &\subseteq \gamma_{m+n}(G)\gamma_{m+n}(G) = \gamma_{m+n}(G). \blacksquare\end{aligned}$$

Problem 3 From Fall 2024 Midterm:

(a) Let G be a finite group and suppose $P, Q \in \mathrm{Syl}_p(G)$ are distinct. Then show that $P \cap N_G(Q) = P \cap Q$.

We know $\mathrm{Syl}_p(N_G(Q)) = \{Q\}$. Also, $P \cap N_G(Q)$ is a p-group in $N_G(Q)$. Hence, by Sylow's second theorem we must have that $P \cap N_G(Q) \subseteq Q$. Since $P \cap N_G(Q) \subseteq P$ as well we know that $P \cap N_G(Q) \subseteq P \cap Q$. And as $Q \subseteq N_G(Q)$ we trivially know that $P \cap Q \subseteq P \cap N_G(Q)$.

(b) Suppose $P \in \mathrm{Syl}_p(G)$ and consider the action of P on $\mathrm{Syl}_p(G)$ by conjugation. Prove that the P-orbit of $Q \in \mathrm{Syl}_p(G)$ (which I'll hereafter denote $P \cdot Q$) has $[P : P \cap Q]$ many elements.

By the orbit-stabilizer theorem we have that $|P \cdot Q| = [P : P_Q]$ where P_Q is the stabilizer of Q. But note that $x \in P$ is in P_Q if and only if $xQx^{-1} = Q$. Hence $P_Q = P \cap N_G(Q) = P \cap Q$.

(c) Let $s_p = |\mathrm{Syl}_p(G)|$. Then suppose $p^e \mid (s_p - 1)$ and $p^{e+1} \not\mid (s_p - 1)$ (where e is some integer). Prove that there are distinct $P, Q \in \mathrm{Syl}_p(G)$ such that $[P : P \cap Q] \leq p^e$.

Suppose $[P : P \cap Q] > p^e$ for all distinct pairs $P, Q \in \mathrm{Syl}_p(G)$. This means by part (b) that if we fix any $P \in \mathrm{Syl}_p(G)$ then the orbit of every $Q \in \mathrm{Syl}_p(G) - \{P\}$ has more than p^e elements. Also note that if $\mathrm{Syl}_p(G)/P$ denotes the set of all P-orbits of the action $P \curvearrowright \mathrm{Syl}_p(G)$ described in part (b), then:

$$s_p = \sum_{P \cdot Q \in \mathrm{Syl}_p(G)/P} |P \cdot Q|$$

This hints at how we can derive a contradiction. Firstly, note that $P \cdot P = \{P\}$. Hence, we can say that:

$$s_p - 1 = \sum_{\substack{P \cdot Q \in \mathrm{Syl}_p(G)/P \\ Q \neq P}} |P \cdot Q|$$

Next note for any $Q \in \mathrm{Syl}_p(G) - \{P\}$ that $|P \cdot Q| = [P : P \cap Q]$ is a power of p. Thus, in order for $|P \cdot Q|$ to have more than p^e elements we must have that $|P \cdot Q| = p^{e+1} p^{k_Q}$ where k_Q is some nonnegative integer. As a result, we can now factor out a p^{e+1} term from the sum above to get that:

$$s_p - 1 = p^{e+1}\Big(\sum_{\substack{P \cdot Q \in \mathrm{Syl}_p(G)/P \\ Q \neq P}} p^{k_Q} \Big)$$

But now we've shown that p^{e+1} divides $s_p - 1$. This is a contradiction. ■

Problem 2 From Fall 2025 Midterm: Suppose G is a finite group and p is a prime divisor of $|G|$. Let P be a Sylow p-subgroup of G and let $x, y \in C_G(P) := \{g \in G : \forall a \in P, ga = ag\}$. Prove that if x and y are conjugate in G then they are conjugate in $N_G(P)$.

Write $y = gxg^{-1}$ where $g \in G$. Then note that since $xa = ax$ for all $a \in P$ we know that $P \subseteq C_G(x)$. Furthermore, since $ya = pa$ for all $a \in P$ we know $gxg^{-1}a = agxg^{-1}$ for all $a \in P$. Equivalently, this means that $xg^{-1}ag = g^{-1}agx$ for all $a \in P$. So, we can conclude that $g^{-1}Pg \subseteq C_G(x)$.

Now we must have that both $P, g^{-1}Pg \in \mathrm{Syl}_p(C_G(x))$. Hence, by Sylow's second theorem there exists $h \in C_G(x)$ such that $hPh^{-1} = g^{-1}Pg$. In turn we know that $P = ghPh^{-1}g^{-1}$. Hence $gh \in N_G(P)$. Also note that $ghxh^{-1}g^{-1} = gxg^{-1} = y$ since $h \in C_G(x)$. ■

Set 7 Problem 3: Suppose G is a finite group and H is a nontrivial subgroup of G.

(a) Show that there exists a function $f : \mathrm{Syl}_p(H) \to \mathrm{Syl}_p(G)$ such that for all $\overline{P} \in \mathrm{Syl}_p(H)$ we have that $\overline{P} = f(\overline{P}) \cap H$. Deduce that $|\mathrm{Syl}_p(H)| \leq |\mathrm{Syl}_p(G)|$.

By Sylow's second theorem, for each $\overline{P} \in \mathrm{Syl}_p(H)$ we can choose some $f(\overline{P}) \in \mathrm{Syl}_p(G)$ such that $\overline{P} \subseteq f(\overline{P})$. Then as $f(\overline{P}) \cap H$ is a p-subgroup in H containing $\overline{P}$, we must have that $f(\overline{P}) \cap H = \overline{P}$. This proves that the function f we want exists.

To show the other inequality, we just note that f is injective. After all, if we know that $f(\overline{P}) = f(\overline{Q})$ then $\overline{P} = f(\overline{P}) \cap H = f(\overline{Q}) \cap H = \overline{Q}$.

(b) Suppose G does not have a non-trivial normal p-subgroup. Then suppose $\overline{P}$ is a non-trivial p-subgroup of G and prove that $|\mathrm{Syl}_p(N_G(\overline{P}))| < |\mathrm{Syl}_p(G)|$.

Note that because $\overline{P}$ is a non-trivial p-subgroup which isn't normal, we know that $\{1\} \subsetneqq N_G(\overline{P}) \subsetneqq G$. Now construct a function $f : \mathrm{Syl}_p(N_G(\overline{P})) \to \mathrm{Syl}_p(G)$ as in part (a). Since we already know f is injective, it suffices to now show that f isn't also surjective.

Suppose for the sake of contradiction that f is a bijection. Then define:

$$O_p(G) \coloneqq \bigcap_{P \in \mathrm{Syl}_p(G)} P.$$

It's easy to see that $O_p(G)$ is a normal p-subgroup of G. Therefore, by assumption we know that $O_p(G) = \{1\}$.

Yet also note that because f is a bijection we know that every $P \in \mathrm{Syl}_p(G)$ is uniquely identified with a group $Q \in \mathrm{Syl}_p(N_G(\overline{P}))$ such that $Q = N_G(\overline{P}) \cap P$. It follows that $O_p(G) \cap N_G(\overline{P}) = O_p(N_G(\overline{P})) = \bigcap_{Q \in \mathrm{Syl}_p(N_G(\overline{P}))} Q$.

Finally, note that that for every $Q \in \mathrm{Syl}_p(N_G(\overline{P}))$ we must have that $\overline{P} \subseteq Q$. After all, we know by Sylow's second theorem that there exists $g \in N_G(\overline{P})$ such that $\overline{P} \subseteq gQg^{-1}$. Equivalently, $\overline{P} = g^{-1}\overline{P}g \subseteq g^{-1}gQg^{-1}g = Q$. This proves that:

$$\overline{P} \subseteq \bigcap_{Q \in \mathrm{Syl}_p(N_G(\overline{P}))} Q \subseteq O_p(G).$$

That contradicts that $O_p(G)$ is trivial since we know that $\overline{P}$ isn't. ■