Problem 40. Prove that an abelian group has a composition series if and only if it is finite.

Proof. ($\Longleftarrow$) If G is finite, it must have order $n = \prod_{i=1}^{m} p_i^{a_i}$ for some distinct primes $p_1, \ldots, p_m$ and $a_0, \ldots, a_m \in \mathbb{Z}^+$. Every subgroup of G are normal since it's abelian, so each each Sylow p_i-subgroup $P_i < G$ of order $p_i^{a_i}$ is normal. So by **Problem 36**, G is the internal direct product $G = P_1 \cdots P_m \cong P_1 \times \cdots \times P_m$ of it's Sylow subgroups. Now consider any $a, b \in P_1 \cdots P_k \setminus P_1 \cdots P_{k-1}$ for some $1 < k \leq m$.

$$[a] = [b] \in P_1 \cdots P_k / P_1 \cdots P_{k-1} \implies b^{-1}a \in P_1 \cdots P_{k-1} \implies |b^{-1}a| \text{ divides } p_1^{a_1} \cdots p_{k-1}^{a_{k-1}}.$$
$$a, b \in P_1 \cdots P_k \setminus P_1 \cdots P_{k-1} = P_k \setminus \{e\} \text{ since } P_1 \cdots P_{k-1} \cap P_k = \{e\}.$$

So $|a|, |b| \in \{p_k^i \mid 1 \leq i \leq a_k\}$ and without loss of generality , $|a| = p_k^{\alpha}$, $|b| = p_k^{\beta}$ for some $0 \leq \alpha \leq \beta \leq a_k$. So then since G is Abelian, $|b^{-1}a|$ divides $\operatorname{lcm}(|a|, |b|) = p_k^{\beta}$. So the $|b^{-1}a|$ divides p_k^{β} and $p_1^{a_1} \cdots p_{k-1}^{a_{k-1}}$, and since $\gcd(p_1^{a_1} \cdots p_{k-1}^{a_{k-1}}, p_k^{\beta}) = 1$, $|b^{-1}a|$ must in fact be 1. So $b^{-1}a = e \implies a = b$. On the other hand, $a = b \implies [a] = [b]$ by definition. Therefore, for any $a, b \in P_1 \cdots P_k \setminus P_1 \cdots P_{k-1}$:

$$[a] = [b] \in P_1 \cdots P_k / P_1 \cdots P_{k-1} \iff a = b.$$

Well, any $g \in P_1 \cdots P_k$ is either in $P_1 \cdots P_k \setminus P_1 \cdots P_{k-1}$ or it isn't, so pick some $q \in P_1 \cdots P_k \setminus P_1 \cdots P_{k-1}$.

$$[g] = \begin{cases} [q], \text{ if } g \in P_1 \cdots P_k \setminus P_1 \cdots P_{k-1} \\ [e], \text{ if } g \in P_1 \cdots P_{k-1} \end{cases}$$

Therefore, $P_1 \cdots P_k / P_1 \cdots P_{k-1} = \{[e], [q]\} \cong \mathbb{Z}_2$ is simple for each $1 < k \leq m$, and by the same sort of argument $P_1 / \{e\}$ is simple since $[a] = [b] \iff b^{-1}a \in \{e\} \iff a = b \implies P_1/\{e\} = \{[e], [g]\}$ for any $g \in P_1 \setminus \{e\}$. So $\{e\} \triangleleft P_1 \triangleleft P_1 P_2 \triangleleft \cdots \triangleleft P_1 P_2 \cdots P_{m-1} \triangleleft P_1 P_2 \cdots P_m = G$ is a composition series. We prove the other direction on the following page.

($\implies$) If an abelian group G has a composition series

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{n-1} \triangleleft H_n = G$$

for some $n \in \mathbb{Z}^+$, then for each $1 \leq k \leq n$, H_k/H_{k-1} is simple and abelian. So then for any $g \in H_k$, $\langle [g] \rangle = \{e\}$ or H_k/H_{k-1}. If $\langle g \rangle = \{e\}$, $\forall g \in H_k/H_{k-1}$, then $H_k/H_{k-1} = \{[e]\}$, otherwise $\exists g_* \in H_k$ such that $\langle [g_*] \rangle = H_k/H_{k-1}$. In either case H_k/H_{k-1} is cyclic. Suppose H_k/H_{k-1} infinite, so $H_k/H_{k-1} \cong \mathbb{Z}$. But then H_k/H_{k-1} isn't simple since $\mathbb{Z}$ isn't simple ($\{e\} \triangleleft 2\mathbb{Z} \triangleleft \mathbb{Z}$), a contradiction. So H_k/H_{k-1} must be a simple finite cyclic group, which implies it has prime order since $H_k \triangleright H_{k-1} \implies |H_k/H_{k-1}| > 1$. Observe.

$$[H_1 : H_0] \in \mathbb{Z}^+ \implies |H_1| = |H_0|[H_1 : H_0] = (1)[H_1 : H_0] \in \mathbb{Z}^+. \text{ Suppose } |H_k| \in \mathbb{Z}^+ \text{ for some } 1 \leq k \leq n.$$
$$\text{Therefore, } |H_{k+1}| = |H_k|[H_{k+1} : H_k] \in \mathbb{Z}^+. \text{ So then } |H_m| \in \mathbb{Z}^+ \text{ for all } 0 \leq m \leq n.$$

So $|H_n| = |G| \in \mathbb{Z}^+$.

Thus,

An abelian group has a composition series if and only if it is finite.

$\square$

Problem 41. Prove that a solvable simple group is abelian.

Proof. Since G is simple, $Z(G) \trianglelefteq G$ is either $\{e\}$ Suppose $Z(G) = \{e\}$, and consider the commutator subgroup $G' = \langle a^{-1}b^{-1}ab \mid a,b \in G\rangle \trianglelefteq G$. $G' \neq \{e\}$, otherwise $a^{-1}b^{-1}ab = e, \forall a,b \in G \implies G$ is abelian $\implies Z(G) = G$, a contradiction. So $G' = G$ and $G^{(2)} = (G')' = (G)' = G' = G$. Now suppose $G^{(k)} = G$ for some $k \geq 2$. Then $G^{k+1} = (G^{(k)})' = (G)' = G' = G$. But then $G^n = G \neq \{e\}$ for all $n \in \mathbb{Z}^+$, and G isn't solvable. So $Z(G) = \{e\}$.

Thus,

A solvable simple group is abelian.

□

We now prove a lemma for **Problem 42**.

Lemma 42. *Any consecutive subquotient of a consecutive quotient of derived subgroups is Abelian.*

Proof. Let $G^{(k-1)} \trianglerighteq H_1 \geq \cdots H_p \geq H_{p+1} \geq H_m \trianglerighteq G^{(k)}$ for some $k,m \in \mathbb{Z}^+$ and $0 \leq p \leq m$. Well, $(H_p)' =$ $\{\}$ □

Problem 43. Prove that a solvable group that has a composition series is finite.

Proof. If a solvable group G with a composition series is abelian, then it is finite by **Problem 40**. Suppose such a group G is not abelian. There exists a minimal $n \in \mathbb{Z}^+$ such that $G^{(n)} = \{e\}$ since G is solvable and we have (i) the derived normal series and (ii) some composition series of G:

$$(i)\ G = G^{(0)} \trianglerighteq G' = G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(n-1)} \trianglerighteq G^{(n)} = \{e\} \text{ and } (ii)\ G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_{m-1} \triangleright H_m = \{e\}$$

By **Schreiers's Theorem** these normal series have an equivalent refinement, that is:

$$(1)\ G_{i,j} = G^{(i+1)}(G^{(i)} \cap H_j) \text{ for } \substack{0 \le j \le n-1 \\ 0 \le j \le m-1} \text{ and } (2)\ H_{i,j} = (G^{(i)} \cap H_j)H_{j+1} \text{ for } \substack{0 \le j \le n \\ 0 \le j \le m-1}$$

$$\implies (3)\ \substack{G=G^0=G_{0,0} \trianglerighteq G_{0,1} \trianglerighteq \cdots \trianglerighteq G_{0,m}=G'=G_{1,0} \trianglerighteq G_{1,1} \trianglerighteq \cdots \trianglerighteq G_{1,m}=G^{(2)}=G_{2,0} \trianglerighteq \cdots \trianglerighteq G_{n-1,m}=G^{(n)}=G_{n,0}=\{e\}. \\ G=H_0=H_{0,0} \trianglerighteq H_{1,0} \trianglerighteq \cdots \trianglerighteq H_{n,0}=H_1=H_{0,1} \trianglerighteq H_{1,1} \trianglerighteq \cdots \trianglerighteq H_{n,1}=H_2=H_{2,0} \trianglerighteq \cdots \trianglerighteq H_{n,m-1}=H_n=H_{0,m}=\{e\}}$$

and (4) $G_{i,j}/G_{i,j+1} \cong H_{i,j}/H_{i+1,j}$

These series are normal by the **Butterfly Lemma** as stated in the class notes. Now, consider any $0 \le k \le n$. We have $H_{k-1} = H_{0,k-1} \trianglerighteq \cdots \trianglerighteq H_{n,k-1} = H_k$ and H_k is a maximal proper normal subgroup of H_{k-1}, that is: $H_k \le N \trianglelefteq H_{k-1} \implies N = H_{k-1}$ or $N = H_k$. So then since we have a containment chain, there exists some $0 \le p \le n$ such that $H_{k-1} = H_{0,k-1} = \cdots = H_{p,k-1} \triangleright H_{p+1,k-1} = \cdots = H_{n,k-1} = H_k$. Therefore, by (4):

$$H_{k-1}/H_k = H_{p,k-1}/H_{p+1,k-1} \cong G_{p,k-1}/G_{p,k}$$

which is abelian by **lemma 1** since it is a subquotient of $G^{(p-1)}/G^{(p)}$. So then H_{k-1}/H_k is abelian and simple, and we proved earlier in **Problem 40** that an abelian simple group must be cyclic and finite of prime order and that if quotients of a composition series of G are finite, that G itself is finite.

Thus,

A solvable group that has a composition series is finite.

$\square$

Problem 45. If $\mathbb{K} \subseteq \mathbb{F}$ is a field extension, $u, v \in \mathbb{F}$, v is algebraic over $\mathbb{K}(u)$, and v is transcendental over $\mathbb{K}$, then u is algebraic over $\mathbb{K}(v)$.

Problem 46. If $\mathbb{K} \subseteq \mathbb{F}$ is a field extension and $u \in \mathbb{F}$ is algebraic of odd degree over $\mathbb{K}$, then so is u^2 and $\mathbb{K}(u) = \mathbb{K}(u^2)$.

Problem 47. Let $\mathbb{K} \subseteq \mathbb{F}$ be a field extension. If $X^n - a \in \mathbb{K}[X]$ is irreducible and $u \in \mathbb{F}$ is a root of $X^n - a$ and m divides n, then the degree of u^m over $\mathbb{K}$ is n/m. What is the irreducible polynomial of u^m over $\mathbb{K}$?.

Problem 48. Let $\mathbb{K} \subseteq R \subseteq \mathbb{F}$ be an extension of rings with $\mathbb{K}, \mathbb{F}$ fields. If $\mathbb{K} \subseteq \mathbb{F}$ is algebraic, prove that R is a field.

Problem 49. Let $f = X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$.

(a) Prove that f is irreducible in $\mathbb{Q}[X]$.

(b) Let u be a real root of f. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(u)$. Express each of the following elements in terms of the basis $\{1, u, u^2\}$ of the $\mathbb{Q}$-vector space $\mathbb{Q}(u)$:

$$u^4, \quad u^5, \quad 3u^5 - u^4 + 2, \quad (u+1)^{-1}, \quad (u^2 - 6u + 8)^{-1}.$$

Problem 50. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find $[F : \mathbb{Q}]$ and a basis of $\mathbb{F}$ over $\mathbb{Q}$.

Proof. To begin, $\sqrt{2}$ and $\sqrt{3}$ are zeros of monic irreducible polynomials $x^2 - 2$ and $x^2 - 3$, respectively, over $\mathbb{Q}$. So $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle \cong (\text{Span}_{\mathbb{Q}}\{1, x\} \subseteq \mathbb{Q}[x]) \cong \mathbb{Q}[x]/\langle x^2 - 3\rangle \cong \mathbb{Q}(\sqrt{3})$. So then $\mathbb{Q}(\sqrt{2}) = \text{Span}\{1, \sqrt{2}\}$ and $\mathbb{Q}(\sqrt{3}) = \text{Span}\{1, \sqrt{3}\}$. Observe.

$$\sqrt{3} = a + b\sqrt{2} \text{ for some } a, b \in \mathbb{Q} \implies 3 = (a + b\sqrt{2})^2 = (a^2 + (2ab)\sqrt{2} + 2b^2) \notin \mathbb{Q},$$

$$\sqrt{2} = a + b\sqrt{3} \text{ for some } a, b \in \mathbb{Q} \implies 2 = (a + b\sqrt{3})^2 = (a^2 + (2ab)\sqrt{3} + 3b^2) \notin \mathbb{Q},$$

$$\sqrt{6} = a + b\sqrt{2} \text{ for some } a, b \in \mathbb{Q} \implies 6 = (a + b\sqrt{2})^2 = (a^2 + (2ab)\sqrt{2} + 2b^2) \notin \mathbb{Q},$$

$$\sqrt{6} = a + b\sqrt{3} \text{ for some } a, b \in \mathbb{Q} \implies 6 = (a + b\sqrt{3})^2 = (a^2 + (2ab)\sqrt{3} + 3b^2) \notin \mathbb{Q}.$$

All of the above are contradictions. So $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ must be linearly independent over $\mathbb{Q}$. Next, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \text{Span}_{\mathbb{Q}(\sqrt{2})}\{1, \sqrt{3}\} = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in \mathbb{Q}(\sqrt{2})\} = \{(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\} = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$. So $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ spans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and since it's elements are linearly independent over $\mathbb{Q}$, it must be a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

Thus,

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} \text{ is a basis for } \mathbb{Q}(\sqrt{2}, \sqrt{3}) \text{ over } \mathbb{Q} \text{ and } [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

$\square$

Problem 51. Let $\mathbb{K}$ be a field. In the field $\mathbb{K}(X)$, let $u = X^3/(X+1)$. What is $[\mathbb{K}(X) : \mathbb{K}(u)]$?

Proof. $(\mathbb{K}(u))(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{K}(u)[t] \right\}$ and then $u = \frac{x^3}{x+1} \implies u(x+1) - x^3 = ux + u - x^3 = 0 \implies x^3 - ux - u = 0$. So x is a zero of the polynomial $t^3 - ut - u$ over $\mathbb{K}(u)$. This means that the degree of x over $K(u)$, or equivalently, $[\mathbb{K}(x) : \mathbb{K}(u)]$ must divide 3. Therefore, $[\mathbb{K}(x) : \mathbb{K}(u)] \in \{1, 3\}$. Suppose $[\mathbb{K}(x) : \mathbb{K}(u)] = 1$, then $\mathbb{K}(x) = \mathbb{K}(u)$ and $x = \frac{f(u)}{g(u)}$ for some $f(u), g(u) \neq 0$ coprime over $\mathbb{K}(u)$. Observe.

$$\begin{aligned}
x^3 - ux - u = (\tfrac{f(u)}{g(u)})^3 - u(\tfrac{f(u)}{g(u)}) - u = 0 \text{ and } & f(u)^3 - uf(u)g(u)^2 - ug(u)^3 = 0. \text{ So then} \\
f(u)^3 &= uf(u)g(u)^2 + ug(u)^3 = ug(u)^2(f(u) + g(u)) \\
&\implies 3\deg(f(u)) = 1 + 2\deg(g(u)) + \max\{\deg(f(u)), \deg(f(u))\}.
\end{aligned}$$

Let $a = \deg(f(u)), b = \deg(g(u))$ and note that both belong to $\mathbb{Z}^+$. We get the following cases:

$$\begin{cases} 3a = 1 + 2b + a \\ \text{or} \\ 3a = 1 + 2b + b \end{cases} \implies \begin{cases} 2a = 1 + 2b \\ \text{or} \\ 3a = 1 + 3b \end{cases} \implies \begin{cases} 2(a+b) = 1 \\ \text{or} \\ 3(a+b) = 1 \end{cases} \implies \begin{cases} (a+b) = \frac{1}{2} \\ \text{or} \\ (a+b) = \frac{1}{3} \end{cases}.$$

Both of the above are contradictions. So $[\mathbb{K}(x) : \mathbb{K}(u)] = 3$.

□

Problem 52. Let $\mathbb{K} \subseteq \mathbb{F}$ be a field extension. If $u, v \in \mathbb{F}$ are algebraic over $\mathbb{K}$ of degrees m and n, respectively, then $[\mathbb{K}(u,v) : \mathbb{K}] \leq mn$. If m and n are relatively prime, then $[\mathbb{K}(u,v) : \mathbb{K}] = mn$.

Proof. $\mathbb{K}(u)$ and $\mathbb{K}(v)$ have bases $\mathcal{B}_u = \{1, \ldots, u^{m-1}\}$ and $\mathcal{B}_v = \{1, \ldots, v^{n-1}\}$, respectively, over $\mathbb{K}$. Also, $\mathbb{K}(u,v) = \text{Span}_{\mathbb{K}_u} \mathcal{B}_v = \{\sum_{i=0}^{n-1} a_i u^i \mid a_0, \ldots, a_{n-1} \in \mathbb{K}(u)\} = \text{Span}_{\mathbb{K}} \mathcal{B}_u \mathcal{B}_v$. So $\mathcal{B}_u \mathcal{B}_v$ span $\mathbb{K}(u,v)$ over $\mathbb{K}$. Therefore, $[\mathbb{K}(u,v) : \mathbb{K}] = |\mathcal{B}_m \mathcal{B}_n| \leq |\mathcal{B}_u||\mathcal{B}_v| = mn$.

Suppose $\gcd(m,n) = 1$. Since $\mathbb{K}(u,v) \supseteq \mathbb{K}(u) \supseteq \mathbb{K}$, by the Tower Law we have:

$$[\mathbb{K}(u,v) : \mathbb{K}] = [\mathbb{K}(u,v) : \mathbb{K}(u)][\mathbb{K}(u) : \mathbb{K}] = [\mathbb{K}(u,v) : \mathbb{K}(v)][\mathbb{K}(v) : \mathbb{K}].$$

Therefore, $[\mathbb{K}(u) : \mathbb{K}] = m$ and $[\mathbb{K}(v) : \mathbb{K}] = n$ both divide $[\mathbb{K}(u,v) : \mathbb{K}]$, which means it is a multiple of both m and n. Well, since $\text{lcm}(m,n) = \frac{mn}{gcd(m,n)} = mn$ and $[\mathbb{K}(u,v) : \mathbb{K}] \leq mn$, it must be the case that in fact $[\mathbb{K}(u,v) : \mathbb{K}] = mn$.

$\square$