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

Proof. hey □

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

Problem 42. Prove that a solvable group that has a composition series is finite.

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 $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle \cong (\mathrm{Span}_{\mathbb{Q}}\{1, x\} \subseteq \mathbb{Q}[x]) \cong \mathbb{Q}[x]/\langle x^2 - 3\rangle \cong \mathbb{Q}(\sqrt{3})$. So then $\mathbb{Q}(\sqrt{2}) = \mathrm{Span}\{1, \sqrt{2}\}$ and $\mathbb{Q}(\sqrt{3}) = \mathrm{Span}\{1, \sqrt{3}\}$. 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, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathrm{Span}_{\mathbb{Q}(\sqrt{2})}\{1, \sqrt{3}\} = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in \mathbb{Q}(\sqrt{2})\} = \{(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\} = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$. 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,

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

□

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 $[\mathbb{K}(x) : \mathbb{K}(u)] = 3$.

$\square$

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

$\square$