Problem 1. If p is a prime number, prove that the nonzero elements of $\mathbb{Z}_p$ form a multiplicative group of order $p-1$. Show that this statement is false if p is not a prime.

Proof. Consider $\mathbb{Z}_4 \setminus \{0\} = \{1,2,3\}$. $2(2) = 0 \notin \mathbb{Z}_4 \setminus \{0\}$, so closure doesn't hold and it can't be a group under multiplication at all. Therefore, the statement is false if p is not prime. Now consider the statement for a prime p.

$\mathbb{Z}_2 = \{0,1\}$ and so $\mathbb{Z}_2^* = \{1\}$ is clearly a group under multiplication of order $2-1=1$. Now consider any prime $p > 2$, which must be odd. $p = 2k+1$ for some $k \in \mathbb{Z}^+$. Observe.

$\langle 2 \rangle_p^* = \{2,4,\ldots,2k\} \sqcup \{2(2k),\ldots\}$. Well, since $p = 2k+1$, $2(2k) = 4k = 2k+2k = (2k+1)+(2k-1) = p+2k-1 = 2k-1 = p-2$. So note that the elements following $2k$ must be odd since p is odd. Additionally, $2q(p-2) = -4q = p-4q$ for $q = 1,\ldots,k-1$ and finally note that $2(k-1)(p-2) = 2(k-1)p - 2(k-1)(2) = p-2k = 1$. Therefore,

$\langle 2 \rangle_p^* = \{2,4,\ldots,2k\} \sqcup \{2(2k),\ldots\} = \{2,4,\ldots,2k\} \sqcup \{p-2, p-4\ldots, p-2k,\ldots\} = \{2,4,\ldots,p-1\} \sqcup \{p-2, p-4,\ldots,1,2,\ldots\}$ and continuing in this fashion loops us back around to the evens.

So, $\langle 2 \rangle_p^* = (\mathcal{E}_p \setminus \{0\}) \sqcup (\mathcal{O}_p) = \mathbb{Z}_p^*$ must therefore be a cyclic multiplicative group of order $p-1$. □

Problem 2.

1. Prove that the relation given by $a \sim b \iff a-b \in \mathbb{Z}$ is an equivalence relation on the additive group $\mathbb{Q}$.
2. Prove that $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group.

Proof.

(a) For any $a,b,c \in \mathbb{Q}$

$[\mathbf{a \sim a}]: \quad a-a = 0 \in \mathbb{Z} \implies a \sim a.$

$[\mathbf{a \sim b \implies b \sim a}]: \quad a \sim b \implies a-b \in \mathbb{Z} \implies -(a-b) = b-a \in \mathbb{Z} \implies b \sim a.$

$[\mathbf{a \sim b, b \sim c \implies a \sim c}]: \quad a \sim b, b \sim c \implies c \sim b \implies (a-b)-(c-b) = a-c \in \mathbb{Z} \implies a \sim c.$

So $\sim$ is an equivalence relation on $(\mathbb{Q},+)$.

(b) $\mathbb{Q}/\mathbb{Z} = \{[q] = q+\mathbb{Z} \mid q \in \mathbb{Q}\}$. Consider any $q_1, q_2 \in (0,1)\cap\mathbb{Q}$. If $[q_1] = [q_2]$, then $[q_1]-[q_2] = \mathbb{Z}$ and $q_1 - q_1 \in \mathbb{Z}$. Well, $q_1, q_2 \in (0,1)$, so $q_1 - q_2 \in (-1,1)\cap\mathbb{Z} \implies q_1 - q_2 = 0$. So $[q_1] = [q_2] \implies q_1 = q_2$. On the other hand, $q_1 = q_2 \implies [q_1] = [q_2]$ by definition. So then

$$q_1 = q_2 \iff [q_1] = [q_2],\ \forall q_1, q_2 \in (0,1)\cap\mathbb{Q}.$$

Since the rationals are dense in $\mathbb{R}$, there are infinitely many distinct rationals in $(0,1)$ and infinitely many distinct cosets of the form $[q]$ where $q \in (0,1)\cap\mathbb{Q}$. Therefore, $\mathbb{Q}/\mathbb{Z}$ is infinite. Lastly, since $(\mathbb{Q},+)$ is Abelian, so is $\mathbb{Q}/\mathbb{Z}$ since $[q_1]+[q_2] = [q_1+q_2] = [q_2+q_1] = [q_2]+[q_1]$.

Thus,

$$\mathbb{Q}/\mathbb{Z} \text{ is an infinite Abelian group.}$$

□

Problem 3. Let p be a prime number and let $\mathbb{Z}(p^\infty)$ be the following subset of the group $\mathbb{Q}/\mathbb{Z}$:

$$\mathbb{Z}(p^\infty) = \{[a/b] \in \mathbb{Q}/\mathbb{Z} \mid a, b \in \mathbb{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}.$$

Prove that $\mathbb{Z}(p^\infty)$ is an infinite subgroup of $\mathbb{Q}/\mathbb{Z}$.

Proof. Clearly, $\mathbb{Z}(p^\infty) \subset \mathbb{Q}/\mathbb{Z}$. Consider any integers $i, j \geq 0$ and let $a_i, a_j \in \mathbb{Z}$.

$$\textbf{[Closure]:} \quad \left[\frac{a_i}{p^i}\right] + \left[\frac{a_j}{p^i}\right] = \left[\frac{p^j(a_i) + p^i(a_j)}{p^{i+j}}\right] \in \mathbb{Z}(p^\infty).$$

$$\textbf{[Inverses]:} \quad \left[\frac{-a_i}{p^i}\right] + \left[\frac{a_i}{p^i}\right] = [0] \implies -\left[\frac{a_i}{p^i}\right] = \left[\frac{-a_i}{p^i}\right].$$

So $\mathbb{Z}(p^\infty) \leq \mathbb{Q}/\mathbb{Z}$. Next, for any $i, j \in \mathbb{Z}^+$, notice that $\frac{1}{p^i}, \frac{1}{p^j} \in (0,1)$. We showed in **Problem 3** that $[q_1] = [q_2] \iff q_1 = q_2, \forall q_1, q_2 \in (0,1)$. Well, if $i \neq j$, then $\frac{1}{p^i} \neq \frac{1}{p^j}$. Therefore, since there are infinitely

many distinct positive integers $k \in \mathbb{Z}^+$, there are infinitely many distinct cosets of the form $\left[\frac{1}{p^k}\right]$ in $\mathbb{Z}(p^\infty)$. Thus,

$$\mathbb{Z}(p^\infty) \text{ is an infinite subgroup of } \mathbb{Q}/\mathbb{Z}.$$

□

Problem 4. If G is a finite group of (non-trivial) even order, prove that G has an element of order two.

Proof. Since G is a group of even order, $|G| = 2n$ for some $n \in \mathbb{Z}^+$. Suppose there does not exist an element of order 2 in G and consider $G \setminus \{e\}$. Since there is no element of order 2, we have that $a \neq a^{-1}$. So then we can form $|G|$ unordered pairs of the form $\{g, g^{-1}\}$, which must be of size 2 since no element is its own inverse. Note that for $a, b \in G$ with $a = b^{-1}$, $b = a^{-1}$ as well. So then $\{a, a^{-1}\} \cup \{b, b^{-1}\} = \{a, b\} \cup \{b, a\} = \{a, b\} = \{b, a\}$. and G must be some disjoint union of distinct unorder pairs of the form $\{g, g^{-1}\}$. That is,

$$G = \bigcup_{g \in G} \{g, g^{-1}\} = \{g_1, g_1^{-1}\} \sqcup \cdots \sqcup \{g_k, g_k^{-1}\}, \text{ for some } k \in \mathbb{Z}^+.$$

Finally, we must have that $2n - 1 = |G| = |\{g_1, g_1^{-1}\} \sqcup \cdots \sqcup \{g_k, g_k^{-1}\}| = 2k$, so an odd equals an even, a contradiction.

Thus,

$$G \text{ has an element of order 2.}$$

□

Problem 5. Let Q_8 be the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Observe that $A^4 = B^4 = I_2$ and $BA = AB^3$. Prove that Q_8 is a group of order 8.

Proof. We will use the notation $-M$ to denote $(-m_{ij})$ where $M = (m_{ij})$. To begin, notice that

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \implies A^3 = A(-I) = -A.$$

We are given that $A^4 = I$, the identity. So $|A| = 4$. Similarly, notice that

$$B^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A^2 = -I,$$

and then obviously $B^{-1} = B^3 = -B$ and we are given that $B^4 = I$, so $|B| = 4$.

So $\langle A \rangle$, $\langle B \rangle \leq Q_8$ are both cyclic subgroups of order 4. Observe.

$$\langle A \rangle \cap \langle B \rangle = \{I, -I\} \implies |\langle A \rangle \langle B \rangle| = \frac{|\langle A \rangle||\langle B \rangle|}{|\langle A \rangle \cap \langle B \rangle|} = \frac{(4)(4)}{(2)} = 8.$$

Well, we are given that A and B generate all of Q_8, which means $Q_8 = \langle A, B \rangle = \langle A \rangle \langle B \rangle$.

Thus,

$$|Q_8| = |\langle A, B \rangle| = |\langle A \rangle \langle B \rangle| = \frac{|\langle A \rangle||\langle B \rangle|}{|\langle A \rangle \cap \langle B \rangle|} = 8.$$

□

Problem 6. Let G be a group and let $\mathrm{Aut}(G)$ denote the set of all automorphisms of G.

1. Prove that $\mathrm{Aut}(G)$ is a group with composition of functions as binary operation.
2. Prove that $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$, $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$, $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ (p prime).

Proof.

(**a**) : Recall that two functions are equal if they share the same domain, codomain, and if they map each element from the domain to the same element in the codomain. Also let $e : G \to G$ denote the identity

mapping $e \coloneqq e(x) = x, \forall x \in G$. Observe. $\forall f,g,h \in \text{Aut}(G),$ and all x

$[\mathbf{e}]: \ (e \circ f)(x) = e(f(x)) = f(x) = f(e(x)) = (f \circ e)(x).$

[Associativity]: $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = (f \circ (g \circ h))(x).$

[Inverses]: Since f is a bijection, it has an inverse function f^{-1} such that$(f \circ f^{-1})(x) = (f^{-1} \circ f)(x)$.

We simply show that this bijection is a group homomorphism. For any $\alpha, \beta \in G, \exists a,b \in G$ such that

$f(a) = \alpha$ and $f(b) = \beta$ and $f(ab) = f(a)f(b) = \alpha\beta,$ since f is a group automorphism. Therefore,

since $f^{-1}(\alpha) = a, f^{-1}(\beta) = b,$ and $f^{-1}(\alpha\beta) = ab,$ we have$f^{-1}(\alpha\beta) = (f^{-1}(\alpha))(f^{-1}(\beta)) = ab = e(ab)$.

So in fact the bijective inverse of any automorphism in $\text{Aut}(G)$ is also an automorphism in $\text{Aut}(G)$.

So $\text{Aut}(G)$ is a group under function composition. □

Problem 7. Let G be an infinite group that is isomorphic to each of its proper subgroups. Prove that $G \cong \mathbb{Z}$.

Proof. Consider any element $g \in G$, and suppose it has finite order m. Then $G \cong \langle g \rangle \cong \mathbb{Z}_m$, a contradiction. So every element of G has infinite order. Once more, consider any $g \in G$. If $G = \langle g \rangle$, then obviously G is cyclic, infinite, and therefore isomorphic to $\mathbb{Z}$. Otherwise $\langle g \rangle < G \implies G \cong \langle g \rangle \cong \mathbb{Z}$, since $\langle g \rangle$ which is is infinite, cyclic, and therefore isomorphic to $\mathbb{Z}$.

Thus,

$$G \cong \mathbb{Z}.$$

□

Problem 8. Let G be the multiplicative group of 2×2 invertible matrices with rational entries. Show that

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

have finite orders but AB has infinite order.

Proof. Note the following products.

$$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \implies A^4 = (-I)^2 = I \tag{1}$$

$$B^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \implies B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \tag{2}$$

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{3}$$

$$(AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \tag{4}$$

Above, by (1) and (2), we see A and B have finite order. Now consider non-trivial powers $n \geq 2$ of (AB).

It is shown in (4) that $(AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. Now suppose $(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ for some $k \geq 2$. Then we have:

$$(AB)^{k+1} = (AB)(AB)^k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}.$$

So we see that $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for all $n \geq 2$ and so in fact it holds for all $n \in \mathbb{N}$ when combined with (3) and the fact that $(AB)^0 = I$. So by definition, AB has infinite order since $(AB)^k \neq I$ for all $k \in \mathbb{Z}^+$.

Thus,

$$A \text{ and } B \text{ have finite order but } AB \text{ has infinite order.}$$

□

Problem 9. Let G be an abelian group containing elements a and b of orders m and n, respectively. Prove that G contains an element of order $\text{lcm}(m,n)$.

Problem 10. Let H,K be subgroups of a group G. Prove that HK is a subgroup of G if and only if $HK = KH$.

Proof.

($\Rightarrow$) $HK \leq G \implies$ For all $hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1} \in HK$. Therefore, $HK = \{hk \mid h \in H, k \in K\} = \{k^{-1}h^{-1} \mid k \in K, h \in H\} = KH$.

($\Leftarrow$) Note $HK = KH \implies \forall hk \in HK, \exists (h_k, k_h) \in H \times K,$ such that $hk = k_h h_k \in KH = HK$. The same logic holds for 'flipped' elements $kh \in KH = HK$. Observe.

[Closure]: $(h_1k_1)(h_2k_2) = (h_1k_1)(k_{h_2}h_{k_2}) = h_1(k_1k_{h_2})h_{k_2} = (k_1k_{h_2})_{h_1}h_{k_1k_{h_2}}h_{k_2} \in KH = HK$.

[Inverses]: For any $hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

So $HK \leq G$.

Thus,

$$HK \leq G \iff HK = KH.$$

□

Problem 11. Let H,K be subgroups of finite index of a group G such that $[G:H]$ and $[G:K]$ are relatively prime. Prove that $G = HK$.

Proof. We begin by proving $(H \cap K) \leq H, K \leq G$.

[1-Step]: $\forall a,b \in (H \cap K)$, $ab^{-1} \in H$ and $ab^{-1} \in K \implies ab^{-1} \in (H \cap K) \implies (H \cap K) \leq H, K \leq G$.

Since $(H \cap K) \leq H, K \leq G$, by the Tower Rule for groups,

$$[G:(H \cap K)] = [G:H][H:H \cap K] = [G:K][K:H \cap K] \implies [K:H \cap K] = \frac{[G:H][H:H \cap K]}{[G:K]}$$
$$\text{and } \gcd([G:H],[G:K]) = 1 \implies [G:K] \mid [H:H \cap K].$$

Now consider $H_K = \{hK \mid h \in H\} \subseteq G/K$ and $H/(H\cap K) = \{h(H\cap K) \mid h \in H\}$. Well,

$$H \ni h_2 \in [h_1]_K \iff h_1K = h_2K \iff h_2^{-1}h_1 \in K \iff h_2^{-1}h_1 \in (H\cap K) \iff h_2 \in [h_1]_{(H\cap K)}$$
$$H \ni h_2 \in [h_1]_{(H\cap K)} \iff h_1(H\cap K) = h_2(H\cap K) \iff h_2^{-1}h_1 \in (H\cap K) \iff h_2^{-1}h_1 \in K \iff h_2 \in [h_1]_K$$

So $h_2 \in [h_1]_K \iff h_2 \in [h_1]_{(H\cap K)}$ and clearly $[h]_K \leftrightarrow [h]_{(H\cap K)}$ is a bijection from H_K to $H/(H\cap K)$. Observe.

$(H_K \subseteq G/K) \iff (|H_k| \leq [G:K])$ and then $(|H_k| \leq [G:K])$ with $([G:K] \mid [H:H\cap K] = |H_K|)$ implies that $|H_K| = [G:K]$. Therefore, $H_k \not\subset G/K$ and we must have that $H_K = G/K$. Therefore, $\forall g \in G, \exists h_g \in H$ such that $gK = h_gK$. Finally, $h_g^{-1}g \in K \implies \exists k_g \in K$ such that $h_g^{-1}g = k_g \implies g = h_gk_g$. So we see that $\forall g \in G$, $\exists (h_g, k_g) \in H \times K$ such that $g = h_gk_g$.

Thus,

$$H, K \leq G \text{ and } \gcd([G:H],[G:K]) = 1 \implies G = HK.$$

□

Problem 12. Let H, K, N be subgroups of G such that $H \subseteq N$. Prove that $HK\cap N = H(K\cap N)$.

Proof. Notice that since $H \subseteq N$, $HN = N$. Therefore, we show $H(K\cap N) = HK\cap HN = HK\cap N$.

$[\subseteq] : \forall a \in H(K\cap N), a = hg$ where $h \in H$ and $g \in (K\cap N)$. Well, $g \in K \implies a = hg \in HK$. Similarly, $g \in N \implies a = hg \in HN$. Therefore, $a \in HK\cap HN \implies H(K\cap N) \subseteq (HK\cap HN) = (HK\cap N)$.

$[\supseteq] : \forall a \in HK\cap HN,\ a = hg$ where $hg \in HK$ and $hg \in HN$. So then $g \in K$ and $g \in N$ and we have $a = hg$ where $h \in H$ and $g \in K\cap N$. Therefore, $a \in H(K\cap N) \implies H(K\cap N) \subseteq HK\cap HN = HK\cap N$.

Thus,

$$H, K, N \leq G \text{ and } H \subseteq N \implies HK\cap N = HK\cap HN = H(K\cap N).$$

□

Problem 13. Let H,K,N be subgroups of G such that $H \subseteq K$, $H \cap N = K \cap N$ and $HN = KN$. Prove that $H = K$.

Proof. $H \subseteq K$ is given. We show $K \subseteq H$ to prove the statement.

$[\supseteq] : \forall k \in K, \exists h_k \in H$ such that $kN = h_k N$ and so $h_k^{-1}k \in N$. Well, $h_k^{-1} \in H \subseteq K$ and therefore by closure $h_k^{-1}k \in K \implies h_k^{-1}k \in (K \cap N) = (H \cap N)$. Finally, $h_k^{-1}k \in H$ and so $\exists h_* \in H$ such that $h_k k = h_* \implies k = h_k h_* \in H$. Therefore, $K \subseteq H$.

Thus,

$$H,K,N \leq G \text{ with } H \subseteq K, H \cap N = K \cap N, \text{ and } HN = KN \implies H = K.$$

□

Problem 14. Let H be a subgroup of G. For $a \in G$, prove that aHa^{-1} is a subgroup of G that is isomorphic to H.

Proof. For any $a \in G$, let $\phi : aHa^{-1} \to H$ be defined via $aha^{-1} \mapsto h$. This mapping is obviously well-defined. Now, for any $h_1, h_2 \in H$,

$$\phi((ah_1a^{-1}))\phi((ah_2a^{-1})) = h_1h_2 = \phi((ah_1h_2a^{-1})) = \phi((ah_1a^{-1})(ah_2a^{-1})).$$

So ϕ is a group homomorphism, which has the trivial kernel $\ker\phi = \{e\}$, and whose image is obviously H. Therefore, by the First Isomorphism Theorem,

$$aHa^{-1} \cong aHa^{-1}/\{e\} = aHa^{-1}/\ker\phi \cong \phi(aHa^{-1}) = H.$$

□

Problem 15. Let G be a finite group and H a subgroup of G of order n. If H is the only subgroup of G of order n, prove that H is normal in G.

Proof. Consider gHg^{-1} for any $g \in G$. By $\square$

Problem 16. If H is a cyclic normal subgroup of a group G, then every subgroup of H is normal in G.

Proof. Suppose $|H| = n$. Since $K \leq H = \langle h \rangle$ where $|h| = n$, K is cyclic by our lemma and there exists some minimal positive power $d \in \mathbb{Z}^+$ of h such that $K = \langle h^d \rangle$. So any $k \in K$ is of the form $k = (h^d)^q$ for some minimal power $q \in \mathbb{Z}^+$. Since $H \trianglelefteq G$,

$$\forall g \in G, gHg^{-1} = H \iff \forall (g, h^q) \in G \times H, \exists h^p \in H, \text{ such that } gh^q g^{-1} = h^p. \text{ for any powers } p, q \in \mathbb{Z}^+$$

Observe.

$$(gh^q g^{-1})^m = \overbrace{(gh^q g^{-1})(gh^q g^{-1}) \cdots (gh^q g^{-1})}^{m} = \overbrace{g(h^{2q} g^{-1})(gh^q g^{-1}) \cdots (gh^q g^{-1})}^{m-1} = \cdots = gh^{mq} g^{-1} = h^{mp}.$$

So then for any $k \in K = \langle h^d \rangle$, where $k = (h^d)^q = (h^q)^d$ and any $g \in G$, $\exists h^p \in H$ such that

$$gh^q g^{-1} = h^p \implies gkg^{-1} = g(h^q)^d g^{-1} = (g(h^q)g^{-1})^d = (h^p)^d = (h^d)^p \in \langle h^d \rangle = K.$$

Note that since $gkg^{-1} = h^{dp}$ implies $gk = h^{dp} g$, there is only one power $(h^d)^p \in K$ for which the equality holds otherwise we get a contradiction. So for each $k_l \in K$, $\exists! k_r \in K$ such that $gk_l g^{-1} = k_r$. To avoid further nightmare indexing, note that we are taking the union of all conjugates $gk_l g^{-1} \in gKg$ on the left side and showing that since each conjugate is paired with some unique $k_r \in K$ on the right side. The union of all conjugates $gk_l g^{-1}$ is equal to the union of all their unique partners k_r and since there are $|K|$ conjugates and $|K|$ unique partners, of course the right side must be all of K.

$$\bigcup_{k_l \in K} gk_l g^{-1} = gKg^{-1} = \bigcup_{gk_l g^{-1} = k_r \in K} k_r = K.$$

Thus,

$$K \leq H = \langle h \rangle \trianglelefteq G \implies K \trianglelefteq G.$$

□

Problem 17. What is $Z(S_n)$ for $n \geq 2$?

Problem 18. If H is a normal subgroup of G such that H and G/H are finitely generated, then G is finitely generated.

Problem 19. If N is a normal subgroup of G, $[G:N]$ is finite, H is a subgroup of G, $|H|$ is finite, and $[G:N]$ and $|H|$ are relatively prime, then H is a subgroup of N.

Problem 20. If N is a normal subgroup of G, $|N|$ is finite, H is a subgroup of G, $[G:H]$ is finite, and $[G:H]$ and $|N|$ are relatively prime, then N is a subgroup of H.

Problem 21. If G is a finite group and H, K are subgroups of G, then

$$[G : H \cap K] \leq [G:H][G:K].$$

Proof. Since G is finite and $H, K \leq G$, we have the following

$$|HK| = \frac{|H||K|}{|H \cap K|} \leq |G| \tag{5}$$

$$[G:H] = \frac{|G|}{|H|} \tag{6}$$

$$[G:K] = \frac{|G|}{|K|} \tag{7}$$

$$\implies [G:H][G:K] = \frac{|G|^2}{|H||K|} \tag{8}$$

$$[G : H \cap K] = \frac{|G|}{|H \cap K|} \tag{9}$$

Observe.

$$|HK| = \frac{|H||K|}{|H\cap K|} \leq |G| \implies (|G|)\frac{|H||K|}{|H\cap K|} \leq |G|^2 \implies (\frac{|G|}{|H||K|})\frac{|H||K|}{|H\cap K|} = \frac{|G|}{|H\cap K|} = [G:K] \leq \frac{|G|^2}{|H||K|} = [G:H][G:K]$$

□

Problem 22. If H,K,L are subgroups of a finite group G such that $H \subseteq K$, then

$$[K:H] \geq [L\cap K : L\cap H].$$

Proof.

Consider elements in $K/H = \{kH \mid k \in K\}$ and $(L\cap K)/(L\cap H) = \{k(L\cap H) \mid k \in (L\cap K)\}$. Well,

$$k_2 \in [k_1]_{(L\cap H)} \implies k_1(L\cap H) = k_2(L\cap H) \implies k_2^{-1}k_1 \in (L\cap H) \implies k_2^{-1}k_1 \in H \implies k_2 \in [k_1]_H$$

Therefore $f : (L\cap K)/(L\cap H) \to K/H$ where $f([k]_{L\cap H}) = [k]_H$ is well-defined. Observe.

$\forall [k_1]_{(L\cap H)}, [k_2]_{(L\cap H)} \in (L\cap K)/(L\cap H)$, if $f([k_1]_{(L\cap H)}) = f([k_2]_{(L\cap H)})$, then $[k_1]_H = [k_2]_H$ by definition. So then $k_2^{-1}k_1 \in H$ and since $[k_1]_{(L\cap K)}, [k_2]_{(L\cap K)} \in (L\cap K)/(L\cap H)$, obviously $k_1, k_2 \in L$. So $k_2^{-1}k_1 \in L$ by closure and finally $k_2^{-1}k_1 \in (L\cap H) \implies [k_1]_{(L\cap H)} = [k_2]_{(L\cap H)}$. So f is injective.

Therefore, since G is finite and f is an injection from $(L\cap K)/(L\cap H)$ to K/H it must be the case that $|(L\cap K)/(L\cap H)| = [L\cap K : L\cap H] \leq [K:H] = |K/H|$. Otherwise, the mapping either wouldn't be well-defined or wouldn't be injective by the Pigeonhole Principle, both contradictions.

Thus,

If H,K,L are subgroups of a finite group G such that $H \subseteq K$, then $[K:H] \geq [L\cap K : L\cap H]$.

□

Problem 23. Let H, K be subgroups of a group G. Assume that $H \cup K$ is a subgroup of G. Prove that either $H \subseteq K$ or $K \subseteq H$.

Proof. $H \cup K \leq G \implies \forall (h,k) \in H \times K,$ we have $hk \in H \cup K$ by closure. Therefore,

$$H \cup K = \{g \mid g \in H \text{ or } g \in K\} \text{ so for each product } hk \in H \cup K \text{ either } hk = g \in H \text{ or } hk = g \in K \text{ or both.}$$

So in fact the only certainty here is that $H \cup K \neq H \sqcup K$ otherwise $hk \notin H \cup K$ which is a subgroup of G. Therefore, necessarily $K \subset H$ or $H \subset K$ or $H = K$.

Thus,

$$H, K, H \cup K \leq G \implies H \subseteq K \text{ or } K \subseteq H.$$

□

Problem 24. Let G be an abelian group, H a subgroup of G such that G/H is an infinite cyclic group. Prove that $G \cong H \times G/H$.

Problem 25. Let P be a Sylow p-subgroup of a finite group G. Prove that $N(N(P)) = N(P)$.

Problem 26. If H is a subgroup of G, prove that the group $N(H)/C(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Proof. Recall that $C(H) = \{g \in G \mid ghg = h, \ \forall h \in H\} \leq N(H) = \{g \in G \mid gHg = H\} \leq G$. **By the notes on 9/12** we have that $C_n : H \to H$ where $C_n(h) = nhn^{-1}$ is an automorphism of H if $n \in N(H)$. Now let $f : N(H) \to \text{Aut}(H)$ where $f(n) = \phi_n, \forall n \in N(H)$. We show f is a group homomorphism. $\forall n_1, n_2 \in N(H)$:

$$f(n_1 n_2) = \phi_{n_1 n_2} := h \mapsto (n_1 n_2) h (n_1 n_2)^{-1} = \phi_{n_1}(n_2 h n_2^{-1}) = \phi_{n_1}(\phi_{n_2}(h)) =: \phi_{n_1} \circ \phi_{n_2} = f(n_1) f(n_2).$$

So f is a group homomorphism from $N(H)$ to $\text{Aut}(H)$. Next, we show that $\ker f = C(H)$.

$(\subseteq)$: $\forall n \in \ker f$, $f(n) = id \in \text{Aut}(H)$. So then $\phi_n(h) = nhn^{-1} = h = id(h), \ \forall h \in H$. Therefore, $n \in C(H)$ and $\ker f \subseteq C(H)$.

$(\supseteq):$ $\forall n \in C(H)$ we have that $nhn^{-1} = h, \forall h \in H$ and so $\phi_n(h) = nhn^{-1} = h = id(h), \forall h \in H$. Therefore, $f(n) = \phi_n = id$, and $n \in \ker f$. So $C(H) \subseteq \ker f$.

We have now shown that $\ker f = C(H)$.

Finally, since f is a group homomorphism from $N(H)$ to $\mathrm{Aut}(H)$, by the **First isomorphism Theorem** we have that $N(H)/\ker f = N(H)/C(H) \cong f(N(H)) \leq \mathrm{Aut}(H)$.

Thus,

$$\text{If } H \leq G, \text{ then } N(H)/C(H) \text{ is isomorphic to some subgroup of } \mathrm{Aut}(H).$$

□

Problem 27. If $G/Z(G)$ is cyclic, then G is abelian.

Proof. Since $G/Z(G)$ is cyclic, $G/Z(G) = \langle [g] \rangle$ for some $g \in G$. Therefore, for any $a, b \in G$,

$$[a] = [g]^{\alpha} = [g^{\alpha}] \text{ for some } \alpha \in \mathbb{N} \tag{10}$$

$$[b] = [g]^{\beta} = [g^{\beta}] \text{ for some } \beta \in \mathbb{N} \tag{11}$$

$$(1) \implies g^{-\alpha} a \in Z(G) \tag{12}$$

$$(2) \implies g^{-\beta} b \in Z(G) \tag{13}$$

So then $g^{-\alpha} a = z_a \implies a = g^{\alpha} z_a$ and $g^{-\beta} b = z_b \implies b = g^{\beta} z_b$ for some $z_a, z_b \in Z(G)$. Observe.

$$ab = (g^{\alpha} z_a)(g^{\beta} z_b) = g^{\alpha} g^{\beta} z_b(z_a) = g^{\beta}(g^{\alpha}) z_b z_a = g^{\beta} z_b (g^{\alpha}) z_a = (g^{\beta} z_b)(g^{\alpha} z_a) = ba.$$

Thus,

$$\text{If } G/Z(G) \text{ is cyclic, then } G \text{ is abelian.}$$

□

Problem 28. Every group of order 28, 56, 200 must contain a normal Sylow subgroup, and hence is not simple.

Proof.

(I): $|G| = 28 = 4(7) = 2^2(7)$. So $|G| = p^2q$ where $p = 2, q = 7$. So by **Problem 35**, G is not simple since it contains a normal Sylow subgroup.

(II): $|G| = 56 = 8(7) = 2^3(7)$. By **Sylow's Theorems**, the number of distinct Sylow $7-$subgroups, n_7, is such that:

$$n_7 \equiv 1 \pmod 7 \text{ and } n_7 \mid 8 \implies n_7 \in \{1,8\}.$$

If $n_7 = 1$, then there is a unique Sylow $7-$subgroup which is therefore normal. So G is not simple since it the Sylow subgroup is proper. If $n_7 = 8$, then there are 8 distinct Sylow $7-$subgroups $P_1, \ldots, P_8$. Since $P_i \cap P_j \leq P_i, P_j$ for any $1 \leq i < j \leq 8$, we have that $|P_i \cap P_j| \in \{1,8\}$ but if it's 8 then the two aren't distinct. So $P_i \cap P_j = \{e\}$ for all $1 \leq i < j \leq 8$. Therefore, $|P_1 \cup \cdots \cup P_8| = 8(7) - 7 = 49$. Therefore, since by the remaining 7 non-identity elements must belong to $Q \setminus \{e\}$, where Q is a Sylow $2-$subgroup, given to exist since $2 \nmid 7$. This is formally justified as follows: Q subgroup only shares identity with any P_i since $g \in Q$ and $g \in P_i$ for all $i = 1, \ldots, 8$. Therefore, $G = P_1 \cup P_8 \cup Q$ implies that Q is a unique Sylow $2-$subgroup, which is therefore normal. So G is not simple.

(III): $|G| = 10(20) = 2(5)(4(5)) = 2^3 5^2$. By **Sylows Theorems**, the number of distinct Sylow $5-$subgroups, n_5, is such that:

$$n_5 \equiv 1 \pmod 5 \text{ and } n_5 \mid 8 \implies n_5 \in \{1,2,4,8\}$$

But $2,4,8 \not\equiv 1 \pmod 5$. So $n_5 = 1$ and the Sylow $5-$subgroup is unique and therefore normal, as well as proper. So G is not simple. □

Problem 29. There is no simple group of order 30.

Proof. $|G| = 36 = 6(6) = 2^2 3^2$. So by **Sylow's Theorems**,

$$n_3 \equiv 1 \pmod 3 \text{ and } n_3 \mid 4 \implies n_3 \in \{1,4\}$$

If $n_3 = 1$ then the proper Sylow $3-$subgroup is unique and therefore normal. So then G is not simple.

If $n_3 = 4$, then there are 4 distinct Sylow $3-$subgroups $P_1, \ldots, P_4$ and they all have pairwise trivial intersections otherwise they aren't distinct. So then $|P_1 \cup \cdots \cup P_4| = 4(3^2) - 3 = |G| - 3$. So then the remaining 3 non-identity elements must belong to the Sylow $2-$subgroup Q of order 4 which exists by **Sylow's Theorems** since $2 \nmid 9$. This is formally justified via $g \in Q \cap P_i \implies |g|$ divides 2^2 and 3^2 which implies that $|g| = 1$ for any $i = 1, \ldots, 4$. Therefore, $|P_1 \cup P_2 \cup P_3 \cup P_4 \cup Q| = 4(3^2) + (4) - 4 = |G| \implies G = P_1 \cup P_2 \cup P_3 \cup P_4 \cup Q$, so Q is a unique Sylow $2-$subgroup, which is therefore normal and since it's proper, G is not simple. □

Problem 30. There is no simple group of order 24.

Proof. $|G| = 4(6) = 2^3(3)$, and so by **Sylow's Theorems**

$$n_2 \equiv 1 \pmod 2 \text{ and } n_2 \mid 3 \implies n_2 \in \{1,3\}$$

If $n_2 = 1$, then the Sylow $2-$subgroup is proper and unique and therefore normal. So G is not simple.

If $n_2 = 3$, then there are 3 distinct Sylow $2-$subgroups P_1, P_2, P_3 which must all have the trivial intersection $\{e\}$ otherwise they are not distinct. Therefore, $|P_1 \cup P_2 \cup P_3| = 3(2^3) - 2 = 22 = |G| - 2$. Therefore the remaining 2 non-identity elements must belong to the Sylow $3-$subgroup Q which exists by **Sylow's Theorems** since $3 \nmid 8$. This is formally justified via $g \in Q \cap P_i \implies |g|$ divides 2^3 and 3 which implies that $|g| = 1$ for any $i = 1, 2, 3$. Therefore, $|P_1 \cup P_2 \cup P_3 \cup Q| = 3(2^3) + 3 - 3 = |G| \implies G = P_1 \cup P_2 \cup P_3 \cup Q$, so Q is a unique Sylow $3-$subgroup, which is therefore normal and since it's proper, G is not simple. □

Problem 31. There is no simple group of order 36.

Proof. $|G| = 36 = 6(6) = 2^2 3^2$. So by **Sylow's Theorems**,

$$n_3 \equiv 1 \pmod 3 \text{ and } n_3 \mid 4 \implies n_3 \in \{1,4\}$$

If $n_3 = 1$ then the proper Sylow $3-$subgroup is unique and therefore normal. So then G is not simple.

If $n_3 = 4$, then there are 4 distinct Sylow $3-$subgroups $P_1, \ldots, P_4$ and they all have pairwise trivial intersections otherwise they aren't distinct. So then $|P_1 \cup \cdots \cup P_4| = 4(3^2) - 3 = |G| - 3$. So then the remaining 3 non-identity elements must belong to the Sylow $2-$subgroup Q of order 4 which exists by **Sylow's Theorems** since $2 \nmid 9$. This is formally justified via $g \in Q \cap P_i \implies |g|$ divides 2^2 and 3^2 which implies that $|g| = 1$ for any $i = 1, \ldots, 4$. Therefore, $|P_1 \cup P_2 \cup P_3 \cup P_4 \cup Q| = 4(3^2) + (4) - 4 = |G| \implies G = P_1 \cup P_2 \cup P_3 \cup P_4 \cup Q$, so Q is a unique Sylow $2-$subgroup, which is therefore normal and since it's proper, G is not simple. □

Problem 32. There is no simple group of order 48.

Proof. $|G| = 4(6) = 2^3(3)$, and so by **Sylow's Theorems**

$$n_2 \equiv 1 \pmod 2 \text{ and } n_2 \mid 3 \implies n_2 \in \{1,3\}$$

If $n_2 = 1$, then the Sylow $2-$subgroup is proper and unique and therefore normal. So G is not simple.

If $n_2 = 3$, then there are 3 distinct Sylow $2-$subgroups P_1, P_2, P_3 which must all have the trivial intersection $\{e\}$ otherwise they are not distinct. Therefore, $|P_1 \cup P_2 \cup P_3| = 3(2^3) - 2 = 22 = |G| - 2$. Therefore the remaining 2 non-identity elements must belong to the Sylow $3-$subgroup Q which exists by **Sylow's Theorems** since $3 \nmid 8$. This is formally justified via $g \in Q \cap P_i \implies |g|$ divides 2^3 and 3 which implies that $|g| = 1$ for any $i = 1, 2, 3$. Therefore, $|P_1 \cup P_2 \cup P_3 \cup Q| = 3(2^3) + 3 - 3 = |G| \implies G = P_1 \cup P_2 \cup P_3 \cup Q$, so Q is a unique Sylow $3-$subgroup, which is therefore normal and since it's proper, G is not simple. □

Problem 33. There is no simple group of order 56.

Proof. $|G| = 56 \implies G$ is not simple by **Problem 28**. □

Problem 34. There is no simple group of order 148.

Proof. $|G| = 4(6) = 2^3(3)$, and so by **Sylow's Theorems**

$$n_2 \equiv 1 \pmod 2 \text{ and } n_2 \mid 3 \implies n_2 \in \{1,3\}$$

If $n_2 = 1$, then the Sylow $2-$subgroup is proper and unique and therefore normal. So G is not simple.

If $n_2 = 3$, then there are 3 distinct Sylow $2-$subgroups P_1, P_2, P_3 which must all have the trivial intersection $\{e\}$ otherwise they are not distinct. Therefore, $|P_1 \cup P_2 \cup P_3| = 3(2^3) - 2 = 22 = |G| - 2$. Therefore the remaining 2 non-identity elements must belong to the Sylow $3-$subgroup Q which exists by **Sylow's Theorems** since $3 \nmid 8$. This is formally justified via $g \in Q \cap P_i \implies |g|$ divides 2^3 and 3 which implies that $|g| = 1$ for any $i = 1,2,3$. Therefore, $|P_1 \cup P_2 \cup P_3 \cup Q| = 3(2^3) + 3 - 3 = |G| \implies G = P_1 \cup P_2 \cup P_3 \cup Q$, so Q is a unique Sylow $3-$subgroup, which is therefore normal and since it's proper, G is not simple. □

Problem 35. Let G be a group of order p^2q where p, q are distinct primes. Show that G is not simple.

Proof. Since p, q are distinct primes, we have two cases.

$(\mathbf{q < p}) \implies n_p \equiv 1 \pmod p$ and $n_p \mid q \implies n_p \in \{1, q\}$. But $2 \leq q < p \implies q \not\equiv 1 \pmod p$. So $n_p = 1$ and G is not simple.

$(\mathbf{p < q}) \implies n_q \equiv 1 \pmod q$ and $n_q \mid p^2 \implies n_q \in \{1, p, p^2\}$. If $n_q = 1$, G is not simple. Next, since $p < q$ we have that $p \not\equiv 1 \pmod q$. Lastly, if $n_p = p^2$, then there are p^2 Sylow $q-$subgroups $Q_1, \ldots, Q_{p^2}$ of order q in G. Therefore, for any $1 \leq i < j < p^2$, since $Q_i \cap Q_j \leq Q_i, Q_j$, we have that $|Q_i \cap Q_j| \in \{1, q\}$. But if $|Q_i \cap Q_j| = q$, then $Q_i = Q_j$ and they are not distinct, a contradiction. So then $Q_i \cap Q_j = \{e\}$ and $Q_1 \cap \cdots \cap Q_{p^2} = \{e\}$. Therefore, $|Q_1 \cup \cdots Q_{p^2}| = p^2q - (p^2 - 1)$. So then the remaining $p^2 - 1$ non-identity elements must belong to the Sylow $p-$subgroup P of order p^2, given to exist by **Sylow's Theorems**. This is formally justified as follows: For any $i = 1, \ldots, p^2$, $Q_i \cap P = \{e\}$ since $g \in Q_i \cap P \implies |g|$ divides q and p^2,

which have $\gcd(q,p^2)=1$ otherwise $q|p^2 \implies q \in \{1,p,p^2\}$ all contradictions since q is prime and $q \nmid p$. So then,

$$|Q_1 \cup Q_{p^2} \cup P| = [p^2(q)-(p^2-1)]+p^2-1 = p^2q \implies G = Q_1 \cup \cdots Q_{p^2} \cup P.$$

Therefore P is a proper and unique Sylow p subgroup, and therefore it is normal. So then $P \triangleleft G$ and G is not simple.

Thus,

A group of order p^2q where p,q are distinct primes is not simple.

□

Problem 36. If every Sylow p-subgroup of a finite group G is normal for every prime p, then G is isomorphic to the direct product of its Sylow subgroups.

Proof. Let P be a Sylow $p-$subgroup of G. If P is normal, then $gPg^{-1} = P, \forall g \in G$. Well, for any Sylow $p-$subgroup Q, we have that there exists $g_* \in G$ such that $Q = g_* P g_*^{-1} = P$. So P is unique. □

Problem 37. If P is a normal Sylow p-subgroup of a finite group G and $f : G \to G$ is a group homomorphism, then $f(P) \subseteq P$.

Proof. Since P is a Sylow $p-$subgroup of G, $|G| = p^n m$ for some $m \in \mathbb{Z}^+$ where $p \nmid m$.

Next, let f_p be f whose domain is restricted to P. f_p is a group homomorphism since for any $a,b \in P$, we have that $f_p(ab) = f(ab) = f(a)f(b) = f_p(a)f_p(b)$. So by the **First Isomorphism Theorem**,

$$P/\ker f_p \cong f_p(P) = f(P).$$

Therefore, $|P/\ker f_p| = \frac{|P|}{|\ker f_p|} = |f(P)| \implies \frac{|P|}{|f(P)|} = |\ker f_p|$ and so $|f(P)|$ divides $|P| = p^n \implies |f(P)| = p^k$ for some $0 \leq k \leq n$. Observe.

$P \trianglelefteq G$ and $f(P) \leq G \implies gP = Pg, \forall g \in G \implies f(P)P = Pf(P) \implies f(P)P \leq G$ by **Problem 10**. Notice that $P \cap f(P)$ must be a $p-$subgroup of G since it is a subgroup of both P and $f(P)$. Therefore, $|f(P)P| = \frac{|f(P)||P|}{|f(P)\cap P|}$ must be some power of p and $f(P)P$ is a $p-$subgroup of G. Lastly, notice that $P \subseteq f(P)P$. Well, $P \not\subset f(P)P$, otherwise $f(P)P$ is a higher order $p-$subgroup of G than the Sylow $p-$subgroup P of G, a contradiction. Therefore $P = f(P)P$ and we must have that $f(P) \subseteq P$.

Thus,

If G is finite, and $P \trianglelefteq G$ is a Sylow p-subgroup and $f : G \to G$ is a group homomorphism, then $f(P) \subseteq P$.

□

Problem 38. Let G be a cyclic group of order n. Let d be a divisor of n. Prove that G has a unique subgroup with d elements.

Proof. If $H = \{e\}$ it is cyclic. If H is non-trivial, then it contains some $h \neq e$. Well, since $h \in H \leq G$, $h = g^k$ for some $k \in \mathbb{Z}^+$. So then there exists some minimal non-trivial power $\mu = \min\{i \in \mathbb{Z}^+ \mid g^i \in H \setminus \{e\}\}$ of g present in $H \setminus \{e\}$. Observe.

By the division algorithm, $\forall m \in \{i \in \mathbb{Z}^+ \mid g^m = H \setminus \{e\}\}$, there exists a unique pair of naturals (q, r) with $0 \leq r < \mu$ such that

$$m = \mu q + r \implies g^m = g^{\mu q + r} = g^{\mu q} g^r \implies g^{m-\mu q} = g^r \in H.$$

Suppose $r \neq 0$. But then $g^r \in H$ for some $0 < r < \mu$ and μ is not minimal, a contradiction. So then $r = 0$ and for any $m \in \mathbb{Z}^+$, such that $g^m \in H$, $g^m = g^{\mu q_*} = (g^\mu)^{q_*}$ for some $q_* \in \mathbb{N}$. Therefore, $H = \langle g^\mu \rangle$, a cyclic group. So any subgroup of a cyclic group is cyclic.

Next, if G is finite and of order n, consider any divisor d of $|G| = n$. Since $G = \langle g \rangle$, $|g| = n$. Well, since $d|n$, $\exists! q \in \mathbb{Z}^+$ such that $dq = n$. So we see $g^{dq} = g^n \implies (g^q)^d = e$. Such a d is necessarily a minimal power that gives identity here since $0 < q, d$ and otherwise there exists $0 < k < n$ such that $k = d'q < dq = n$, and so $g^k = e$ and $|g| = k$, a contradiction. So $|g^q| = d$. Suppose $|g^{q'}| = d$ for some $q' \leq n$ with $q' \neq q$. But then

$n = q'd < qd = n$, a contradiction. So there is only one power q of g with order d. Since any $d-$ordered subgroup H_d of G is cyclic, it must be generated by some power of G, of which there is only one and so $H_d = \langle g^d \rangle$ is the only subgroup of order d which divides n. □

Problem 39. A semidirect product $H \rtimes_\varphi K$ is unchanged up to isomorphism if the action $\varphi : K \to \mathrm{Aut}(H)$ is composed with an automorphism of K. More precisely, for automorphisms $f : K \to K$, prove that $H \rtimes_{\varphi \circ f} K \cong H \rtimes_\varphi K$.

Proof. Let $\phi : H \rtimes_\varphi K \to H \rtimes_{\varphi \circ f} K$ be defined via $(h,k) \mapsto (h, f^{-1}(k))$. Since $\phi^{-1} := (h,k) \mapsto (h, f(k))$ is such that $\phi^{-1}(\phi((h,k))) = \phi^{-1}((h, f^{-1}(k))) = (h, f(f^{-1}(k))) = (h,k)$ and $\phi(\phi^{-1}(h,k)) = \phi((h, f(k))) = (h, f^{-1}(f(k))) = (h,k)$, ϕ has an inverse and is a bijection. We now show ϕ is a group homomorphism.

$$\phi((h_1,k_1)(h_2,k_2)) = \phi(h_1\varphi_{k_1}(h_2), k_1k_2) = (h_1\varphi_{k_1}(h_2), f^{-1}(k_1k_2)) = (h_1\varphi_{k_1}(h_2), f^{-1}(k_1k_2)) =$$
$$(h_1\varphi_{f(f^{-1}(k_1))}(h_2), f^{-1}(k_1)f^{-1}(k_2)) = (h_1, f^{-1}(k_1))(h_2, f^{-1}(k_2)) = \phi((h_1,k_1))\phi((h_2,k_2)).$$

Thus, ϕ is a group isomorphism and $H \rtimes_{\varphi \circ f} K \cong H \rtimes_\varphi K$. □

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 is 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 its 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 $\mathrm{lcm}(|a|, |b|) = p_k^\beta$. 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 $\{e\} \triangleleft P_1 \triangleleft P_1P_2 \triangleleft \cdots \triangleleft P_1P_2\cdots P_{m-1} \triangleleft P_1P_2\cdots P_m = G$ 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.

□

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 $Z(G) = G$.

Thus,

A solvable simple group is abelian.

□

Problem 42. 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:

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

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

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

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: $H_k \trianglelefteq N \trianglelefteq H_{k-1} \implies N = H_{k-1}$ 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.

□

Problem 43. If G is a finite group and H is a normal subgroup of G, prove that G has a composition series where one of its terms is H.

Problem 44. Let G be a solvable group and H a nontrivial normal subgroup of G. Prove that G has a nontrivial normal subgroup A such that A is contained in H and A is abelian.

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

Proof. v is algebraic over $\mathbb{K}(u) \implies$ there exists a non-zero degree $n \in \mathbb{Z}^+$ polynomial $P(x) = \sum_{i=0}^{n} p_i(u)x^i$ over $\mathbb{K}(u)$ such that $P(v) = 0$. Let $m = \max\{\deg(p_i(x)) \mid 0 \leq i \leq n\}$. Then for each $0 \leq i \leq n$, we have that $p_i(x) = \sum_{j=0}^{m} a_{ij}x^j$ for some $a_{i0}, \ldots, a_{im} \in \mathbb{K}$. Note that if $\deg p_i(x) < m$, $a_{i(\deg p_i(x))} = \cdots = a_{im} = 0$. Observe.

$$\begin{aligned} P(v) &= \sum_{i=0}^{n} p_i(u)v^i = \sum_{i=0}^{n}(\sum_{j=0}^{m} a_{ij}u^j)v^i = \sum_{i=0}^{n}(\sum_{j=0}^{m} a_{ij}v^iu^j) = \sum_{i=0}^{n}(a_{i0}v^j + a_{i1}v^ju + \cdots + a_{im}v^ju^m) \\ &= \sum_{i=0}^{n} a_{i0}v^j + \sum_{i=0}^{n} a_{i1}v^ju + \cdots + \sum_{i=0}^{n} a_{im}v^ju^m = \sum_{j=0}^{m}(\sum_{i=0}^{n} a_{ij}v^iu^j) = \sum_{j=0}^{m} q_j(v)u^j = Q(u) = 0, \end{aligned}$$

where $q_j(x) = \sum_{i=0}^{n} a_{ij}x^j$ and $Q(x) = \sum_{j=0}^{m} q_j(v)x^j \in \mathbb{K}(v)[x]$.

Now, by definition not all a_{ij}'s are zero, so not all $q_j(x)$'s are zero. That is, there exists some $0 \leq k \leq m$ such that $q_k(x) \neq 0 \in \mathbb{K}[x]$. Well, since v is transcendental over $\mathbb{K}$, $q_k(x) \neq 0 \implies q_k(v) \neq 0$; v cannot be a zero of $q_k(x)$ since it's non-zero over $\mathbb{K}$. Therefore, $Q(x) = \sum_{j=0}^{m} q_j(v)x^j \neq 0 \in \mathbb{K}(v)[x]$ and since $Q(u) = 0$, u must be algebraic over $\mathbb{K}(v)$.

Thus,

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

Proof. Since u is algebraic of odd degree $n = 2k+1$ over $\mathbb{K}$ for some $k \in \mathbb{Z}^+$,

$$\mathbb{K}[x]/\langle P(x)\rangle \cong \text{Span}\{1, x, \ldots, x^{n-1}\} \cong \text{Span}\{1, u, \ldots, u^{n-1}\} = \mathbb{K}(u)$$

for some monic irreducible degree n polynomial $P(x)$ over $\mathbb{K}$ such that $p(u) = 0$. (This isomorphism is the canonical one $[f(x)] \longleftrightarrow f(u)$ where $[f(x)] = [g(x)] \longleftrightarrow f(u) = g(u)$. Therefore, $[0] = [P(x)] \longleftrightarrow 0 \implies P(u) = 0 \in \mathbb{K}(u)$. This is also just given since the extension is defined by that relation but whatever.) Obviously, $u^2 \in \mathbb{K}(u)$, so any $q(u^2)$ belongs to $\mathbb{K}(u)$ and therefore any $\frac{f(u^2)}{g(u^2)} \in \mathbb{K}(u^2)$ also belongs to $\mathbb{K}(u)$. So $\mathbb{K}(u^2) \subseteq \mathbb{K}(u)$. Additionally, u^2 must be algebraic otherwise $\mathbb{K}(u^2) \cong K(x) \supset K[x] = \text{Span}\{x^m \mid m \in \mathbb{N}\}$ is infinite dimensional and so $\mathbb{K}(u^2) \subseteq \mathbb{K}(u^2)$ implies that $\mathbb{K}(u)$ is infinite dimensional, a contradiction. Next, $P(x) = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{2k+1} a_i x^i = \sum_{i=0}^{k} a_{2i+1} x^{2i+1} + \sum_{i=0}^{k} a_{2i} x^{2i} = x\sum_{i=0}^{k} a_{2i+1} x^{2i} + \sum_{i=0}^{k} a_{2i} x^{2i}$ for some $a_0, \ldots, a_{2k+1} \in \mathbb{K}$. So then $P(u) = u\sum_{i=0}^{k} a_{2i+1} u^{2i} + \sum_{i=0}^{k} a_{2i} u^{2i} = 0$. Since $\sum_{i=0}^{k} a_{2i+1} u^{2i}$ has degree $2k < n$, u can't be a zero of it since it is degree n over $\mathbb{K}$. Therefore,

$$u = \frac{-\sum_{i=0}^{k} a_{2i} u^{2i}}{\sum_{i=0}^{k} a_{2i+1} u^{2i}} = \frac{-\sum_{i=0}^{k} a_{2i} (u^2)^i}{\sum_{i=0}^{k} a_{2i+1} (u^2)^i} \in \left\{ \frac{f(u^2)}{g(u^2)} \mid f(x), g(x) \in \mathbb{K}[x] \text{ and } g(u^2) \neq 0 \right\} = \mathbb{K}(u^2).$$

So then any $f(u) \in \mathbb{K}(u)$ must also belong to $\mathbb{K}(u^2)$ and $\mathbb{K}(u) \supseteq \mathbb{K}(u^2)$.

Thus,

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

Proof. Since $u^n - a = 0$ and $m \mid n, n = mk$ for some $k \in \mathbb{Z}^+$ and so $u^{mk} - a = 0 \implies (u^m)^k - a = 0$, so u^m is a zero of $x^k - a \in \mathbb{K}[x]$. Now, suppose $x^k - a$ is reducible over $\mathbb{K}$. Then $x^k - a = f(x)g(x)$ for some non-constant polynomials $f(x), g(x) \in \mathbb{K}[x]$ such that $\deg(f(x)) = \alpha$, $\deg(g(x)) = \beta$ and $\alpha + \beta = k$. So we get that $x^n - a = (x^m)^k - a = f(x^m)g(x^m)$.

(The composition $(a \circ b)(x) = a(b(x))$ over a field $\mathbb{F}$ can only (1) multiply $b(x)$ by itself some finite number of times and/or (2) scale $b(x)$ via $\mathbb{F}$ and/or (3) add scalars in $\mathbb{F}$ to $b(x)$ all of which preserve structure.)

So $f(x^m)$ and $g(x^m)$ are polynomials of degree $m\alpha > 1$, and $m\beta > 1$, respectively. But then $x^n - a$ is reducible over $\mathbb{K}$, a contradiction. So $x^k - a$ must be irreducible over $\mathbb{K}$ and u^m is a zero of it.

Thus,

if $\mathbb{K} \supseteq \mathbb{F}$ is a field extension, $X^n - a \in \mathbb{K}[X]$ is irreducible, $u \in \mathbb{F}$ is a root of $X^n - a$, and m divides n, then the degree of u^m over $\mathbb{K}$ is n/m and $x^k - a$ is the irreducible polynomial of u^m over $\mathbb{K}$.

□

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

Proof. Since $\mathbb{K}$ is algebraic over $\mathbb{F}$, $\forall \alpha \in \mathbb{K}$ there exists a minimal non-zero polynomial $f(\alpha)$ over $\mathbb{F}$ such that $f(\alpha) = 0$. Therefore, since $R \subseteq \mathbb{K}$, it must also be algebraic over $\mathbb{F}$. If $\mathbb{K} = R = \mathbb{F} = \{0\}$, they're... arguably fields but then $\mathbb{K}$ can't be algebraic over $\mathbb{F}$ since there are no non-zero polynomials over $\mathbb{F}$. So $R \neq \{0\}$ and it contains some non-zero element $r \in R \subseteq \mathbb{K}$. It has a multiplicative inverse r^{-1} in $\mathbb{K}$ and there exists some minimal degree $n \in \mathbb{Z}^+$ polynomial $P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ such that $P(r) = 0$. Note that since it's irreducible and $r \neq 0$, the constant term is non-zero, otherwise it's reducible: $\sum_{i=0}^{n} a_i x^i = \sum_{i=1}^{n} a_i x^i =$

$x(\sum_{i=0}^{n} a_i x^{i-1})$. Observe.

$$P(r) = \sum_{i=0}^{n} a_i r^i = 0 \implies r^{-1}(\sum_{i=0}^{n} a_i r^i) = 0 \implies r^{-1}a_0 + \sum_{i=0}^{n} a_i r^{i-1} = 0$$
$$\implies r^{-1}a_0 = -\sum_{i=0}^{n} a_i r^{i-1} \implies r^{-1} = -\frac{1}{a_0}\sum_{i=0}^{n} a_i r^{i-1} \in R.$$

This holds because $\mathbb{F} \subseteq R$. So then every $r \in R$ has a multiplicative inverse r^{-1} in R. So then since R has multiplicative inverses, it has unity by closure, and it is commutative with no zero divisors via $R \subseteq \mathbb{K}$, R is a field.

Thus,

if $\mathbb{K} \supseteq R \supseteq \mathbb{F}$ is an extension of rings where $\mathbb{K}$ and $\mathbb{F}$ are fields, and $\mathbb{K} \supseteq \mathbb{F}$ is algebraic, then R is a field.

□

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

1. Prove that f is irreducible in $\mathbb{Q}[X]$.
2. 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, u^5, $3u^5 - u^4 + 2$, $(u+1)^{-1}$, $(u^2 - 6u + 8)^{-1}$.

Proof. **(a)** 3 is prime and divides all integer coefficients of $f(x) = x^3 - 6x^2 + 9x + 3 \in \mathbb{Q}[x]$ except the leading one, and $3^2 \nmid 3$, the constant term of $f(x)$, so by **Eisenstein's Criterion** $f(x)$ is irreducible over $\mathbb{Q}$.

(b) Since $f(x) = x^3 - 6x^2 + 9x + 3$ is monic and irreducible over $\mathbb{Q}$ and u is a zero of it we have

$$\mathbb{Q}[x]/\langle x^3 - 6x^2 + 9x + 3\rangle \cong \mathbb{Q}(u) = \text{Span}\{1, u, u^2\} \text{ and } u^3 - 6u^2 + 9u + 3 = 0.$$

So then $u^3 = 6u^2 - 9u - 3$. Observe.

$$u^4 = u(u^3) = u(6u^2 - 9u - 3) = 6u^3 - 9u^2 - 3u = 6(6u^2 - 9u - 3) - 9u^2 - 3u = 27u^2 - 57u - 18.$$

$$u^5 = u(u^4) = u(27u^2 - 57u - 18) = 27u^3 - 57u^2 - 18u = 27(6u^2 - 9u - 3) - 57u^2 - 18u.$$

$$= 105u^2 - 261u - 81.$$

$$3u^5 - u^4 + 2 = 3(105u^2 - 261u - 81) - (27u^2 - 57u - 18) + 2 = 288u^2 - 726u - 223.$$

Next, we use long division to factor $f(u)$ into a multiple of $(u+1)$ and $(u^2 - 6u + 8)$ so we can solve for the using the remainder. We could have solved a system but this is easier.

$$\begin{array}{rrrl|l} x^3 & -6x^2 & +9x & +3 & x+1 \\ \cline{5-5} -x^3 & -x^2 & & & x^2-7x+16 \\ \cline{1-2} & -7x^2 & +9x & & \\ & 7x^2 & +7x & & \\ \cline{2-3} & & 16x & +3 & \\ & & -16x & -16 & \\ \cline{3-4} & & & -13 & \end{array}$$

So $\frac{f(u)}{u+1} = u^2-7u+16-\frac{13}{u+1} \implies f(u) = 0 = (u^2-7u+16)(u+1)-13 \implies \frac{1}{13}(u^2-7u+16)(u+1) = 1$.

So $(u+1)^{-1} = \frac{1}{13}(u^2-7u+16)$.

Next we solve for $(u^2-6u+8)^{-1}$.

Division didn't work so we just solve a system directly. $(u^2-6u+8)^{-1} = au^2+bu+c$ for some $a,b,c \in \mathbb{Q}$.

So $(u^2-6u+8)(u^2-6u+8)^{-1} = (u^2-6u+8)(au^2+bu+c) = au^4+(b-6a)u^3+(c-6b+8a)u^2+(-6c+8b)u+8c = (c-a)u^2+(-3a-b-6c)u+(-3b+8c) = 0u^2+0u+1$.

$$\begin{pmatrix} -1 & 0 & 1 & 0 \\ -3 & -1 & -6 & 0 \\ 0 & -3 & 8 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & \frac{1}{35} \\ 0 & 1 & 0 & -\frac{9}{35} \\ 0 & 0 & 1 & \frac{1}{35} \end{pmatrix}.$$

$$\implies a = \tfrac{1}{35}, \quad b = -\tfrac{9}{35}, \quad c = \tfrac{1}{35}.$$

So, $(u^2-6u+8)^{-1} = \frac{1}{35}(u^2-9u+1)$. □

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

$\text{Span}\{1,\sqrt{2}\}$ 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,

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

□

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

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.

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

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

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

Problem 53. Let $K \subseteq F$ be a field extension. Prove that F is algebraic over K if and only if for every intermediary field $K \subseteq E \subseteq F$, every K-embedding $\sigma : E \to E$ is an isomorphism.

Problem 54. If $f \in K[X]$ (K field) has degree n and F is a splitting field of f over K, prove that $[F : K] \mid n!$.

Proof. If f has a degree 1 over $\mathbb{K}$, then it has only one zero a whose minimal polynomial must have degree $1 = [\mathbb{K}(a) : \mathbb{K}] = [\mathbb{F} : \mathbb{K}] \mid 1!$. If f has degree 2 over $\mathbb{K}$, then it has at most two distinct zeros. Suppose f is redicuble. Then it splits into two linear factors over $\mathbb{K}$ and so $\mathbb{F} \cong \mathbb{K} \implies [\mathbb{F} : \mathbb{K}] = 1 \mid 2!$. Otherwise f is irreducible, and so the minimal polynomial for a zero a_1 of f must be of the form $\frac{f(x)}{\ell}$ for some $\ell \in \mathbb{K}$, and

therefore both zeros a_1 and a_2 share the same minimal polynomial $x^2+bx+c=(x-a_1)(x-a_2)\in\mathbb{K}[x]$. So then $x^2-(a_1+a_2)x+a_1a_2=x^2+bx+c \implies a_2=-b-a_1\in\mathbb{K}(a)$ and so $\mathbb{F}\cong\mathbb{K}(a) \implies [\mathbb{F}:\mathbb{K}]\in\{1,2\}$ both of which divide 2!. Suppose $[\mathbb{F}:\mathbb{K}]\mid d!$ if $\mathbb{F}$ is the splitting field of any degree d polynomial f over $\mathbb{K}$ for all $1\leq d<m$ for some $m\geq 2$. Consider the statement for a degree m polynomial f over $\mathbb{K}$.

If f is reducible, then $f(x)=P(x)Q(x)$ for some non-constant degree p and $(m-p)$ polynomials P and Q over $\mathbb{K}$. Let $\mathbb{F}_P$ be the splitting field of P over $\mathbb{K}$ and $\mathbb{F}_Q$ be the splitting field of Q over $\mathbb{F}_P$. Since $\deg_{\mathbb{K}}(P(x))=p, deg_{\mathbb{F}_P}(Q(x))=deg_{\mathbb{K}}(Q(x))=m-p<m$, we have that $[\mathbb{F}_Q:\mathbb{F}_P]\mid(m-p)!$ an $[\mathbb{F}_P:\mathbb{K}]\mid p!$. Well, $\mathbb{F}_Q=(\mathbb{F}_P)(\alpha\mid Q(\alpha)=0)\cong(\mathbb{K}(a\mid P(a)=0))(b\mid Q(b)=0)=\mathbb{K}(\alpha\mid P(\alpha)=0 \text{ or } Q(\alpha)=0)\cong\mathbb{F}$. So finally, $\mathbb{F}_Q\supseteq\mathbb{F}_P\supseteq\mathbb{K} \implies [\mathbb{F}:\mathbb{K}]=[\mathbb{F}_Q:\mathbb{K}]=[\mathbb{F}_Q:\mathbb{F}_P][\mathbb{F}_P:\mathbb{K}]\mid p!(m-p)!\mid m!$ (via $\binom{p}{m}=\frac{m!}{p!(m-p)!}$). So $[\mathbb{F}:\mathbb{K}]\mid m!$.

If f is irreducible, then for any zero a of f, $[\mathbb{K}(a):\mathbb{K}]=m$ and by the division algorithm we have $f(x)=(x-a)Q(x)$ over $\mathbb{K}(a)$ where Q has degree $m-1$. Since Q has degree less than m, the splitting field $\mathbb{F}_Q$ of Q over $\mathbb{K}(a)$ must be such that $[\mathbb{F}_Q:\mathbb{K}(a)]\mid(m-1)!$ and since $\mathbb{F}_Q=(\mathbb{K}(a))(\alpha\mid Q(\alpha)=0)=\mathbb{K}(\alpha\mid x-\alpha=0 \text{ or } Q(\alpha)=0)\cong\mathbb{F}$ we have that $[\mathbb{F}:\mathbb{K}]=[\mathbb{F}_Q:\mathbb{K}]=[\mathbb{F}_Q:\mathbb{F}_P][\mathbb{F}_P:\mathbb{K}]$ divides $m(m-1)!=m!$.

Thus, by induction,

> If $\mathbb{F}\supseteq\mathbb{K}$ is the splitting field of a degree $n\in\mathbb{Z}^+$ polynomial over $\mathbb{K}$, then $[\mathbb{F}:\mathbb{K}]\mid n!$.

□

Problem 55. If $K\subseteq F$ is a field extension, F is algebraically closed, and E consists of all elements of F that are algebraic over K, then E is an algebraic closure of K.

Proof. All elements of $\mathbb{E}=\{\alpha\in\mathbb{F}\mid\alpha \text{ is algebraic over } \mathbb{K}\}$ are algebraic over $\mathbb{K}$. Now, consider some polynomial $f(x)$ over $\mathbb{K}$. $\mathbb{F}\supseteq\mathbb{K} \implies \mathbb{F}[x]\supseteq\mathbb{K}[x] \implies f(x)\in\mathbb{F}$ and since $\mathbb{F}$ is algebraically closed, any zero a of $f(x)$ must belong to $\mathbb{F}$. So any algebraic a over $\mathbb{K}$ belongs to $\{\alpha\in\mathbb{F}\mid\alpha \text{ is algebraic over } \mathbb{K}\}=\mathbb{E}$.

Next, we prove that $\mathbb{E}$ is a field. For any $\alpha, \beta \in \mathbb{E} \subseteq \mathbb{F}$ with $\beta \neq 0$,

$$\begin{aligned}
&\alpha\beta^{-1}, \alpha - \beta \in \mathbb{K}(\alpha, \beta) \implies \mathbb{K}(\alpha, \beta, \alpha\beta^{-1}) = \mathbb{K}(\alpha, \beta, \alpha - \beta) = \mathbb{K}(\alpha, \beta) \\
&\implies \mathbb{Z}^+ \ni [\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta, \alpha\beta^{-1}) : \mathbb{K}(\alpha\beta^{-1})][\mathbb{K}(\alpha\beta^{-1}) : \mathbb{K}] \\
&\implies \mathbb{Z}^+ \ni [\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta, \alpha - \beta) : \mathbb{K}(\alpha - \beta)][\mathbb{K}(\alpha - \beta) : \mathbb{K}] \\
&\implies [\mathbb{K}(\alpha\beta^{-1}) : \mathbb{K}], [\mathbb{K}(\alpha - \beta) : \mathbb{K}] \in \mathbb{Z}^+
\end{aligned}$$

Therefore, since adjoining $\alpha\beta^{-1}$ or $\alpha - \beta$ to $\mathbb{K}$ gives a finite extension of K, they must algebraic over $\mathbb{K}$, and so they both belong to $\mathbb{E}$, which is then a subfield of $\mathbb{F}$. Additionally, since every element of $\mathbb{E}$ is algebraic over $\mathbb{K}$, $\mathbb{E}$ is an algebraic extension of $\mathbb{K}$. Lastly, consider any $g(x) = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{E}[x]$. Since $\mathbb{E}$ is algebraic over $\mathbb{K}$, $\alpha_0, \ldots, \alpha_n$ are all algebraic over $\mathbb{K}$. So then any zero β of $g(x)$ is algebraic over $\mathbb{K}(\alpha_0, \ldots, \alpha_n)$, which must be a finite extension of $\mathbb{K}$. Observe.

$$\begin{aligned}
&\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) \supseteq \mathbb{K}(\beta) \supseteq \mathbb{K} \text{ and } [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}(\alpha_0, \ldots, \alpha_n)] \in \mathbb{Z}^+ \\
&\implies [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}(\alpha_0, \ldots, \alpha_n)][\mathbb{K}(\alpha_0, \ldots, \alpha_n) : \mathbb{K}] \in \mathbb{Z}^+ \\
&\implies \mathbb{Z}^+ \ni [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}(\beta)][\mathbb{K}(\beta) : \mathbb{K}]
\end{aligned}$$

So $[\mathbb{K}(\beta) : \mathbb{K}] \in \mathbb{Z}^+ \implies \beta$ is algebraic over $\mathbb{K}$. Therefore, $\beta \in \mathbb{E}$ and $\mathbb{E}$ is an algebraically closed, algebraic extension of $\mathbb{K}$. Thus,

$$\mathbb{E} \text{ is an algebraic closure of } \mathbb{K}.$$

□

Problem 56. No finite field K is algebraically closed.

Problem 57. If $[F : K] = 2$, then $K \subseteq F$ is a normal extension.

Proof. Let $P(x) \in \mathbb{K}[x]$ be irreducible over $\mathbb{K}$ with a zero $\alpha \in \mathbb{F}$. The minimal polynomial $P_\alpha(x) \in \mathbb{K}[x]$ of

α must divide $P(x)$, and since $P(x)$ is irreducible over $\mathbb{K}$, $P_\alpha(x) = \frac{1}{c}P(x)$, where c is the leading coefficient of $P(x)$. Well, $\alpha \in \mathbb{F} \implies \mathbb{F} \supseteq \mathbb{K}(\alpha) \supseteq \mathbb{K}$. Therefore,

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}(\alpha)][\mathbb{K}(\alpha) : \mathbb{K}] = 2 \implies \alpha \text{ has degree 1 or 2 over } \mathbb{K}.$$

If α has degree 1 over $\mathbb{K}$, $P_\alpha(x)$ and therefore $P(x)$ has only one zero, α which belongs to $\mathbb{F}$. If α has degree 2 over $\mathbb{K}$, then $P_\alpha(x)$ and therefore $P(x)$ has at most two distinct roots α, β such that $P_\alpha(x) = x^2 + bx + c = (x-\alpha)(x-\beta)$. for some $b, c \in \mathbb{K}$. So then $x^2 + bx + c = (x-\alpha)(x-\beta) = x^2 - (\beta+\alpha)x + \alpha\beta = x^2 + bx + c$. Finally, $\beta + \alpha = -b \implies \beta = b - \alpha \in \mathbb{F}$. In either case, $P(x)$ splits completely over $\mathbb{F}$. So then any irreducible polynomial over $\mathbb{K}$ with a root in $\mathbb{F}$ splits completely over $\mathbb{F}$.

Thus,

$$\text{If } [\mathbb{F} : \mathbb{K}] = 2, \text{ then } \mathbb{K} \subseteq \mathbb{F} \text{ is a normal extension.}$$

□

Problem 58. If d is a non-negative rational number, then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}))$ is the identity or is isomorphic to $\mathbb{Z}_2$.

Proof. If $\sqrt{d} \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ and so the only automorphism of $\mathbb{Q}$ that fixes $\mathbb{Q}$ is the identity, that is, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d})) = \{\mathrm{id}\} \cong \{e\}$. If $\sqrt{d} \notin \mathbb{Q}$, then it's minimal polynomial must be $x^2 - d \in \mathbb{Q}[x]$, and so it's only conjugate roots are $\sqrt{d}, -\sqrt{d}$. Any automorphism in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$ is completely defined by where it's adjoined root $\sqrt{d}$ is sent to, and since it may only be sent to it's conjugates $\sqrt{d}, \sqrt{-d}$ via $\mathrm{id} \coloneqq \sqrt{d} \mapsto \sqrt{d}$ and $\phi \coloneqq \sqrt{d} \mapsto -\sqrt{d}$, respectively, we have that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d})) = \{\mathrm{id}, \phi\} \cong \mathbb{Z}_2$.

Thus,

$$\text{If } d \text{ is a nonnegative rational number, then } \mathrm{Aut}_{\mathbb{Q}}\big(\mathbb{Q}(\sqrt{d})\big) \text{ is the identity or is isomorphic to } \mathbb{Z}_2.$$

□

Problem 59. What is the Galois group of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ over $\mathbb{Q}$?

Proof. By the previous proof, $d \in \mathbb{Q} \setminus \mathbb{Q}^-$ and $\sqrt{d} \notin \mathbb{Q} \implies \sqrt{d}, -\sqrt{d}$ are the only conjugate roots of $\sqrt{d}$ over $\mathbb{Q}$. So then since any automorphism in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ is completely defined by which conjugates over $\mathbb{Q}$ it's adjoined roots are permuted to, and each root has two conjugates, we have that $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})| = 2^3 = 8$. Let $\phi_d \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ be the automorphism that sends $\sqrt{d}$ to $-\sqrt{d}$ and fixes all other roots, for each $d \in \{2,3,5\}$.

Any such ϕ_d^2 sends $\sqrt{d}$ to $-\sqrt{d}$ and then back to $\sqrt{d}$, and since it fixes everything else $\phi_d^2 = \mathrm{id}$ for each $d \in \{2,3,5\}$. By definition, these are distinct automorphisms which must generate the group, that is, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}) = \langle \phi_2, \phi_3, \phi_5 \rangle$. Well, $\phi_a \circ \phi_b \coloneqq \begin{smallmatrix} \sqrt{a} \mapsto -\sqrt{a} \\ \sqrt{b} \mapsto -\sqrt{b} \end{smallmatrix} = \phi_b \circ \phi_a$ for each distinct pair $a,b \in \{2,3,5\}$, since these automorphisms don't affect generators other than the one, regardless of order. So then since all generators of the group commute pairwise, they all commute with each other in general and we have that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ is an abelian group of order 8 with three distinct elements of order 2.

Thus,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

Problem 60. Assume that K is a field of characteristic zero. Let G be the subgroup of $\mathrm{Aut}_K(K(X))$ that is generated by the K-automorphism induced by $X \mapsto X+1$. Prove that G is an infinite cyclic group. What is the fixed field E of G? What is $[K(X) : E]$?

Proof. Let $\phi \in \mathrm{Aut}_{\mathbb{K}}\big(\mathbb{K}(x)\big)$ be the $\mathbb{K}$-automorphism defined above, so $G = \langle \phi \rangle$. Now suppose G is finite of order $n \in \mathbb{Z}^+$. Then, $\phi^n \coloneqq x \mapsto x+n = \mathrm{id} \coloneqq x \mapsto x$, that is, $n = 0$ over $\mathbb{K}$. In fact since $|G| = n$, $k \neq 0$ for all $0 < k < n$. But then $\mathrm{Char}\,\mathbb{K} = n \in \mathbb{Z}^+$, a contradiction. So G must be an infinite cyclic group.

By definition, $\mathbb{E} = \mathrm{Fix}_{\mathbb{K}(x)}(G) = \{\frac{f(x)}{g(x)} \in \mathbb{K}(x) \mid \sigma(\frac{f(x)}{g(x)}) = \alpha,\ \forall \sigma \in G\}$. Consider any $Q(x) = \frac{f(x)}{g(x)} \in \mathbb{K}(x)$ which is fixed by G where $f(x), g(x)$ have $k, c \in \mathbb{N}$ distinct zeros over $\mathbb{K}$, respectively. (The base field $\mathbb{K}$ is always fixed by any subset of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$ where $\mathbb{E}$ is an extension of $\mathbb{K}$, so this is an assumption we can make.) Then $Q(x)$ has at most k zeros and at most c poles.

Suppose $Q(x)$ has a zero $\alpha \in \overline{\mathbb{K}}$, for some fixed algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, we must have that $Q(\alpha) = \phi^k(\alpha) = Q(\alpha + k) = 0$, $\forall k \geq 1$, and so Q has infinitely many zeros in $\overline{\mathbb{K}}$, a contradiction. So $Q(x)$ must not have any zeros. Next, notice that if $Q(x)$ is fixed by G, then so is $Q^{-1}(x) = \frac{g(x)}{f(x)}$. So then suppose $Q(x)$ has some pole $\beta \in \overline{\mathbb{K}}$. It is a zero of $Q^{-1}(x)$. But then once again we have that $Q^{-1}(\beta) = \phi_k(Q^{-1}(\beta)) = Q^{-1}(\beta + k) = 0$, $\forall k \geq 1$, and so $Q^{-1}(x)$ infinitely many poles in $\overline{\mathbb{K}}$, a contradiction. So then $Q(x)$ must have no poles.

Therefore, since $Q(x)$ has no poles or zeros, it must be some quotient which belongs to $\mathbb{K}$. So $\mathbb{E} \subseteq \mathbb{K}$. On the other hand, $G \subseteq \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(x))$ fixes $\mathbb{K}$ by definition, so $\mathbb{K} \subseteq \mathbb{E}$. Therefore, $\mathbb{E} = \mathbb{K}$ is the fixed field of G. and since $\mathbb{E} = \mathbb{K}$, we must have that $K(x)$ has infinite dimension over $\mathbb{E} = \mathbb{K}$. □

Problem 61. Let k be a finite field of characteristic $p > 0$.

1. Prove that for every $n > 0$ there exists an irreducible polynomial $f \in k[X]$ of degree n.
2. Prove that for every irreducible polynomial $P \in k[X]$ there exists $n \geq 0$ such that P divides $X^{p^n} - X$.

Proof. **(a)** We use the convention $\mathbb{K} = \mathbb{F}_{p^n}$ for some $n \in \mathbb{Z}^+$ since $\Bbbk$ is a finite field of characteristic p. By our theorems, there exists an extension $\mathbb{K}_m = \mathbb{F}_{p^{nm}}$ of degree m over $\mathbb{F}_{p^n}$. Suppose that for all $\alpha \in \mathbb{F}_{p^{nm}}$, the degree of α over $\mathbb{K}$ is strictly less than $[\mathbb{F}_{p^{nm}} : \mathbb{F}_{p^n}] = m$. So then by our theorems, any such α must belong to $\mathbb{F}_{p^n}(\alpha) \subset \mathbb{F}_{p^{nm}}$ and $[\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_{p^n}] = d$ for some divisor $0 < d < nm$ of $[\mathbb{F}_{p^{nm}} : \Bbbk_n] = nm$. Once again, by our theorems, this must be the unique subfield $\mathbb{F}_{p^d}$ of order p^d. So then all elements of $\mathbb{F}_{p^{nm}}$ must belong to some unique proper subfield $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^{nm}}$ where $d \mid nm$.

Let $\{d_1, \ldots, d_k\}$ be the set of all divisors of nm that are less than nm, and let $d_{\max}$ be the maximal divisor of nm. By our theorems, we have the containment chain $\mathbb{F}_{p^{d_1}} \subset \mathbb{F}_{p^{d_2}} \subset \cdots \subset \mathbb{F}_{p^{d_{\max}}} \subset \mathbb{F}_{p^{nm}}$ and so in fact all elements of $\mathbb{F}_{p^{nm}}$ belong to $\mathbb{F}_{p^{d_{\max}}}$. But then $\mathbb{F}_{p^{d_{\max}}}$ isn't proper, a contradiction. Therefore, there exists an element $\alpha_m \in \mathbb{F}_{p^{nm}}$ with degree m over $\mathbb{F}_{p^n}$, and so there exists a monic irreducible polynomial of α_m over $\mathbb{F}_{p^n}$ with degree m, that is $\mathbb{F}_{p^{nm}} = \mathbb{F}_{p^{nm}}(\alpha_m)$. So for every $m > 0$ there exists an irreducible polynomial of degree m over $\mathbb{K} = \mathbb{F}_{p^n}$.

(b) Now, consider any irreducible polynomial $P(x) \in \mathbb{F}_{p^n}[x]$. It must have some degree $q \in \mathbb{Z}^+$, and some zero α with the minimal polynomial $P_\alpha(x) = \frac{P(x)}{a} \in \mathbb{F}_{p^n}[x]$ where a is the leading coefficient of $P(x)$. So

then α has degree q over $\mathbb{F}_{p^n}$ and $[\mathbb{F}_{p^n}(\alpha):\mathbb{K}]=q$. Therefore, by our theorems, $\mathbb{F}_{p^n}(\alpha)=\mathbb{F}_{p^{nq}}$, the splitting field of $f_{p,n,q}(x)=x^{p^{nq}}-x$ over $\mathbb{F}_p$. Well, $\alpha\in\mathbb{F}_{p^{nq}} \implies |\alpha|.$ divides $|\mathbb{F}^*_{p^{nq}}|=p^{nq}-1$ and so $\alpha^{p^{nq}-1}=1 \implies \alpha^{p^{nq}}=\alpha \implies f_{p,n,q}(\alpha)=(\alpha)^{p^{nq}}-\alpha=0$. So α is a zero of $f_{p,n,q}(x)=x^{p^{nq}}-x$ over $\mathbb{F}_p$, which is also a polynomial over $\mathbb{F}_{p^n}$. Therefore, for every irreducible polynomial of degree q over $\mathbb{K}=\mathbb{F}_{p^n}$ divides $x^{p^{nq}}-x$. □

Problem 62. Let p be a prime and $\mathbb{F}_q$ (where $q=p^s$) be the finite field with q elements. Let $f\in\mathbb{F}_q[X]$ be an irreducible polynomial. Prove that f is irreducible in $\mathbb{F}_{q^m}[X]$ if and only if m and the degree of f are relatively prime.

Proof. Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_{p^n}$ with degree $\deg f(x)=d$ for some prime p and some $n\geq 1$. Also, let $f_{p,N}(x)=x^{p^N}-x$ over $\mathbb{F}_p$ for any $N\in\mathbb{Z}^+$ and recall that every element of $\mathbb{F}_{p^{nN}}$, the splitting field of $f_{p,N}(x)$, is a zero of $f_{p,N}(x)$.

Now, since $f(x)$ is irreducible over $\mathbb{F}_{p^n}$, any zero α of $f(x)$ has the minimal polynomial $p_\alpha(x)=\frac{f(x)}{c}$ over $\mathbb{F}_{p^n}$ where c is the leading coefficient of $f(x)$ and so it has degree d over $\mathbb{F}_{p^n}$. That is, $\mathbb{F}_{p^n}(\alpha)=\mathbb{F}_{p^{nd}}$. So then α is a zero of $f_{p,nd}(x)$, and we also have that d is smallest integer such that $\alpha^{p^{nd}}=\alpha$. Furthermore, $\alpha^{nk}=\alpha \iff d\mid k$.

($\implies$) If $f(x)$ is irreducible over $\mathbb{F}_{p^{nm}}$, then α has degree d over both $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^{nm}}$. So $\alpha=k_1=k_2$ is the smallest integer such that $\alpha^{p^{nk_1}}=\alpha^{p^{nmk_2}}=\alpha$. Additionally, the previous equalities hold for any multiples $k_1,k_2\geq 1$ of d. Suppose $g=\gcd(d,m)>1$, then $\frac{d}{g}=\ell_d<d$, $\frac{m}{g}=\ell_m<m$. Observe.

$$m\ell_d=m\frac{d}{g}=\frac{m}{g}d=d\ell_m \implies \alpha^{p^{nm\ell_d}}=\alpha^{p^{nm(\frac{d}{g})}}=\alpha^{p^{nd(\frac{m}{g})}}=\alpha^{p^{nd\ell_m}}=\alpha.$$

But then there is a smaller positive integer $k_2=\ell_d<d$ such that $\alpha^{nmk_2}=\alpha$, a contradiction. So we must have that $\gcd(d,m)=1$.

($\impliedby$) On the other hand, if $\gcd(d,m)=1$, recall that that d is the smallest positive integer $d=k_1$ such that $\alpha^{p^{nk_1}}=\alpha$ for any zero α of $f(x)$. So for any $k_2\geq 1$ such that $\alpha^{p^{nmk_2}}=\alpha$, we must have that $d\mid mk_2$. Suppose we have such a k_2 less than d. But then $\gcd(d,m)=1$ and $d\mid mk_2 \implies d\mid k_2$ and $k_2<d$, which is

impossible. So the smallest such $k_2 = d$, which is also the degree of α over $\mathbb{F}_{p^{nm}}$. Since degree of any zero α of $f(x)$ is d over $\mathbb{F}_{p^{nm}}$, $f(x)$ must be irreducible over $\mathbb{F}_{p^{nm}}$. (Otherwise we have some minimal polynomial of degree less than d which can be pulled out of $f(x)$ over $\mathbb{F}_{p^{nm}}$). □

Problem 63. Prove that $E = \mathbb{F}_2[X]/(X^4 + X^3 + 1)$ is a field with 16 elements. What are the roots of $X^4 + X^3 + 1$ in E?

Proof. Let $p(x) = x^4 + x^3 + 1 \in \mathbb{F}_2$. $p(0) = p(1) = 1 \neq 0$, so $P(x)$ has no zeros in $\mathbb{F}_2$ and therefore no linear factors over $\mathbb{F}_2$, and so it can't factor into a linear and cubic. Suppose $P(x)$ is reducible. Then must split into two irreducible quadratics over $\mathbb{F}_2$. Well, $x^2 + 1 = (x+1)(x-1)$ and $x^2 + x = x(x+1)$, and $x^2 = x(x)$ over $\mathbb{F}_2$. Since $x^2 + x + 1$ is the only irreducible quadratic over $\mathbb{F}_2$, we must have that $P(x) = (x^2 + x + 1)^2$. Recall that Char $\mathbb{F}_2 = 2$ and so $(f(x) + g(x))^2 = (f(x))^2 + (g(x))^2$ over $\mathbb{F}_2$. But then

$$P(x) = x^4 + x^3 + 1 = ((x^2) + (x+1))^2 = x^4 + (x+1)^2 = x^4 + x^2 + 1, \text{ a contradiction.}$$

So then $P(x) = x^4 + x^3 + 1$ is irreducible of degree 4 over $\mathbb{F}_2$ and for any zero α of $P(x)$

$$\mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle = \text{Span}_{\mathbb{F}_2}\{[1],[x],[x^2],[x^3]\} \cong \text{Span}_{\mathbb{F}_2}\{1, \alpha, \alpha^2, \alpha^3\} = \mathbb{F}_2(\alpha).$$

So $\mathbb{E} = \mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle$ is a 4-dimensional $\mathbb{F}_2$-vector space and we must have that $|\mathbb{E}| = 2^4 = 16$. For the remainder of this proof we will exclusively work in $\mathbb{E}$ and so we refer to cosets $[f(x)]_{\mathbb{E}}$ by any of their representatives $f(x)$ and let modulo $x^4 + x^3 + 1$ be implied.

So $\mathbb{E} = \text{Span}\{1, x, x^2, x^3\}$ and since $x^4 + x^3 + 1 = 0$ in this field, $x^4 = -x^3 - 1 = x^3 + 1$, and obviously x is a root of $p(x) = x^4 + x^3 + 1$ over $\mathbb{E}$. Then, recall that since $\mathbb{E} \cong \mathbb{F}_{2^4}$, is a finite field extension of $\mathbb{F}_2$ with characteristic 2, we must have that the Frobenius mapping $\varphi_2 \coloneqq x \mapsto x^2$ is an endomorphism of $\mathbb{E}$ (In fact it is a isomorphism in $\text{Aut}_{\mathbb{F}_2}(\mathbb{F}_{2^4})$) and so it permutes roots of polynomials in $\mathbb{E}[x]$ to each other. Well, $x^4 = x^3 + 1 \implies x^5 = x(x^4) = x(x^3 + 1) = x^4 + x = x^3 + x + 1 \implies x^6 = x(x^5) = x(x^3 + x + 1) = x^4 + x^2 + x = (x^3 + 1) + x^2 + x = x^3 + x^2 + x + 1$.

Therefore, the orbit $\text{Orb}_{\varphi_2}(\mathbb{E}) = \{x\} \cup \{x^2\} \cup \{x^4 = x^3 + 1\} \cup \{x^8 = (x^4)^2 = (x^3+1)^2 = x^6 + 1 = (x^3 + x^2 + x + 1) + 1 = x^3 + x^2 + x\} \cup \cdots = \{x, x^2, x^3 + 1, x^3 + x^2 + x\}$ must be all roots of $P(x) = x^4 + x^3 + 1$ over $\mathbb{E}$, since they are four distinct elements and $P(x)$ has at most four distinct roots. □

Problem 64. Prove that an algebraic extension of a perfect field is a perfect field.

Proof. Let $\mathbb{K}$ be a perfect field. If $\mathbb{K}$ has characteristic 0, then so does any extension of it since they share 1, and so any algebraic extension of $\mathbb{K}$ must be perfect.

If $\mathbb{K}$ has characteristic $p > 0$. Since $\mathbb{K}$ is perfect, every irreducible polynomial $f(x)$ over $\mathbb{K}$ has no repeated roots in some splitting field $\mathbb{F}_{f(x)}$ of $f(x)$. That is, the minimal polynomial of any algebraic element has no repeated linear factors in $\mathbb{F}_{P(x)}$.

Therefore, if $\mathbb{E}$ is some algebraic extension of $\mathbb{K}$, then any $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{K}$. It's minimal polynomial $P_{\alpha,\mathbb{K}}(x)$ over $\mathbb{K}$ has no repeated roots some splitting field $\mathbb{F}_{P(x)}$ of $P(x)$. Now, since α is a zero of $P_{\alpha,\mathbb{K}}(x)$ which also belongs to $\mathbb{E}[x]$, the minimal polynomial $P_{\alpha,\mathbb{E}}(x)$ of α over $\mathbb{E}$ must divide $P_{\alpha,\mathbb{K}}(x)$ over $\mathbb{E}$. Therefore, $P_{\alpha,\mathbb{E}}(x)$ must split completely over $\mathbb{F}_{P(x)}$ into distinct linear factors as well, since otherwise $P_{\alpha,\mathbb{K}}(x)$ is divisible by some repeated linear factor of $P_{\alpha,\mathbb{E}}(x) \mid P_{\alpha,\mathbb{K}}(x) \in \mathbb{F}_{P(x)}[x]$, a contradiction. So every minimal polynomial over $\mathbb{E}$ is seperable. Since every irreducible polynomial over $\mathbb{E}$ is simply some minimal polynomial of one of it's zeros, which we proved is seperable, scaled by some $c \in \mathbb{E}$, every irreducible over $\mathbb{E}$ is also seperable. Therefore, $\mathbb{E}$ is perfect. □

Problem 65. Show that extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ is Galois. Find its Galois group.

Proof. $\sqrt[4]{2}$ and i have minimal polynomials $x^4 - 2$ and $x^2 + 1$ over $\mathbb{Q}$ they are both algebraic over $\mathbb{Q}$ and so $\mathbb{Q}(\sqrt[4]{2}, i)$ is a finite, and therefore algebraic extension of $\mathbb{Q}$. Since $\mathbb{Q}$ has characteristic 0, it is perfect, and so is any algebraic extension of it such as $\mathbb{Q}(\sqrt[4]{2}, i)$. So then $\mathbb{Q}(\sqrt[4]{2}, i)$ is seperable.

Now, notice that $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ are all zeros of $x^4 - 2$. Well, $x^4 - 2$ has at most 4 distinct zeros over $\mathbb{C}$, and so these must be all of them. Well, any extension $\mathbb{E}$ where $x^4 - 2$ splits completely over must

contain i and $\sqrt[4]{2}$, so $\mathbb{Q}(\sqrt[4]{2},i) \subseteq \mathbb{E}$. Therefore, $\mathbb{Q}(\sqrt[4]{2},i)$ must be a splitting field for x^4-2. Therefore, since $\mathbb{Q}(\sqrt[4]{2},i)$ is a splitting field of some polynomial over $\mathbb{Q}$, it is normal. Finally, since $\mathbb{Q}(\sqrt[4]{2},i)$ is seperable and normal, it must be Galois. Now, since x^4-2 is monic and irreducible over $\mathbb{Q}(i)$, $[\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i)]=4$ and $|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})| = [\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i)][\mathbb{Q}(i):\mathbb{Q}] = 8$.

Let $a=\sqrt[4]{2}$ and $b=i$. So the conjugates of a are $\{a,-a,ba,-ba\}$ and the conjugates of b are $\{b,-b\}$. Also recall that that $a^4=(\sqrt[4]{2})^4=2$ and $b^2=i^2=-1$. Now, we denote automorphisms in $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(a,b)/\mathbb{Q})$ that sends an adjoined root $\alpha \in \{a,b\}$ to one of its conjugates α' and fixes the other adjoined root via $\phi_{\alpha,\alpha'} \coloneqq \alpha \mapsto \alpha$. Observe.

$$\phi_{b,-b}^2 \coloneqq \phi_{b,-b}(\phi_{b,-b}(b)) = \phi_{b,-b}(-b) = b \implies \phi_{b,-b}^2 = \mathrm{id}.$$

$$(\phi_{b,-b}\circ\phi_{a,ba})(a) = \phi_{b,-b}(ba) = -ba \neq ba = \phi_{a,ba}(a) = (\phi_{a,ba}\circ\phi_{b,-b})(a)$$

$$\implies \phi_{b,-b}\circ\phi_{a,ba} \neq \phi_{a,ba}\circ\phi_{b,-b}$$

Therefore, $\mathrm{Gal}(\mathbb{Q}(a,b)/\mathbb{Q})$ is a non-abelian group of order 8 with an element $\phi_{b,-b}$ of order 2. So then since it could only be isomorphic to Q_8 or D_4 purely by order, and Q_8 has no elements of order 2, we must have that $\mathrm{Gal}(\mathbb{Q}(a,b)/\mathbb{Q}) \cong D_4$. □

Problem 66. Let k be a field of characteristic $p>0$, $f=X^p-X+a \in k[X]$ an irreducible polynomial and α a root of f in an algebraic closure $\bar{k}$ of k. Show that the extension $k \subseteq k(\alpha)$ is Galois. Find the Galois group $G(k(\alpha)/k)$.

Problem 67. Find all the subfields of the splitting field of $(X^2+3)(X^2-5)$ over $\mathbb{Q}$.

Problem 68. Show that the equation

$$X(X^2-4)(X^2+2)=2$$

cannot be solved by radicals over $\mathbb{Q}$.

Problem 69. Let $\varepsilon \in \mathbb{C}$ be a primitive root of $X^5-1 \in \mathbb{Q}[X]$. Find the Galois group $G(\mathbb{Q}(\varepsilon)/\mathbb{Q})$, all its subgroups, and all the subfields of $\mathbb{Q}(\varepsilon)$. Express $\cos\pi/5$ and $\cos 2\pi/5$ by using radicals.