Austin Mohr
Math 740 Homework

In the problems below, let $A$ and $B$ be two classes and let $R$ be a binary relation with $R \subseteq A \times B$. For $X \subseteq A$ and $Y \subseteq B$, put

$$X^{\rightarrow} = \{b \mid xRb \text{ for all } x \in X\}$$
$$Y^{\leftarrow} = \{a \mid aRy \text{ for all } y \in Y\}$$

Problem 0

Prove that if $W \subseteq X \subseteq A$, then $X^{\rightarrow} \subseteq W^{\rightarrow}$. (Likewise, if $V \subseteq Y \subseteq B$, then $Y^{\leftarrow} \subseteq V^{\leftarrow}$.)

*Proof.*

$$\begin{aligned} y \in X^{\rightarrow} &\Rightarrow aRy \text{ for all } a \in X \\ &\Rightarrow aRy \text{ for all } a \in W \text{ (as } W \subseteq X) \\ &\Rightarrow y \in W^{\rightarrow} \end{aligned}$$

Therefore, $X^{\rightarrow} \subseteq W^{\rightarrow}$.

Similarly,

$$\begin{aligned} x \in Y^{\leftarrow} &\Rightarrow xRb \text{ for all } b \in Y \\ &\Rightarrow xRb \text{ for all } b \in V \text{ (as } V \subseteq Y) \\ &\Rightarrow x \in V^{\leftarrow} \end{aligned}$$

Therefore, $Y^{\leftarrow} \subseteq V^{\leftarrow}$. □

Problem 1

Prove that if $X \subseteq A$, then $X \subseteq X^{\rightarrow\leftarrow}$. (Likewise, if $Y \subseteq B$, then $Y \subseteq Y^{\leftarrow\rightarrow}$.)

*Proof.* Let $x \in X$. By definition,

$$X^{\rightarrow} = \{b \mid aRb \text{ for all } a \in X\}$$

Hence, $xRb$ for all $b \in X^{\rightarrow}$. Also by definition, we have that

$$X^{\rightarrow\leftarrow} = \{a \mid aRb \text{ for all } b \in X^{\rightarrow}\},$$

and so $x \in X^{\rightarrow\leftarrow}$. Therefore, $X \subseteq X^{\rightarrow\leftarrow}$.

Similarly, let $y \in Y$. By definition,

$$Y^{\leftarrow} = \{a \mid aRb \text{ for all } b \in Y\}$$

Hence, $aRy$ for all $a \in Y^{\leftarrow}$. Also by definition, we have that

$$Y^{\leftarrow\rightarrow} = \{b \mid aRb \text{ for all } a \in Y^{\leftarrow}\},$$

and so $y \in Y^{\leftarrow\rightarrow}$. Therefore, $Y \subseteq Y^{\leftarrow\rightarrow}$. □

Problem 2

Prove that $X^{\rightarrow\leftarrow\rightarrow} = X^{\rightarrow}$ for all $X \subseteq A$. (Likewise, $Y^{\leftarrow\rightarrow\leftarrow} = Y^{\leftarrow}$ for all $Y \subseteq B$.)

*Proof.* As $X \subseteq A$, problem 1 gives that

$$X \subseteq X^{\rightarrow\leftarrow}.$$

Combining this with the result of problem 0, we see that

$$X^{\rightarrow\leftarrow\rightarrow} \subseteq X^{\rightarrow}.$$

Now, as $X^{\rightarrow} \subseteq B$, problem 1 gives that

$$X^{\rightarrow} \subseteq X^{\rightarrow\leftarrow\rightarrow}.$$

Therefore, $X^{\rightarrow\leftarrow\rightarrow} = X^{\rightarrow}$.

Similarly, as $Y \subseteq B$, problem 1 gives that

$$Y \subseteq Y^{\leftarrow\rightarrow}.$$

Combining this with the result of problem 0, we see that

$$Y^{\leftarrow\rightarrow\leftarrow} \subseteq Y^{\leftarrow}.$$

Now, as $Y^{\leftarrow} \subseteq A$, problem 1 gives that

$$Y^{\leftarrow} \subseteq Y^{\leftarrow\rightarrow\leftarrow}.$$

Therefore, $Y^{\leftarrow\rightarrow\leftarrow} = Y^{\leftarrow}$. □

Problem 3

Prove that the collection of subclasses of $A$ of the form $Y^{\leftarrow}$ is closed under the formation of arbitrary intersections (as is the collection of subclasses of $B$ of the form $X^{\rightarrow}$). We call classes of the form $Y^{\leftarrow}$ and of the form $X^{\rightarrow}$ closed.

*Proof.* Let $\{Y_\alpha \mid \alpha \in I\}$ be a family of subsets of $B$ for some indexing set $I$. If $\bigcap_{\alpha\in I} Y_\alpha^{\leftarrow}$ is empty, then the claim holds trivially, as

$$\bigcap_{\alpha\in I} Y_\alpha^{\leftarrow} = \emptyset^{\leftarrow}.$$

Otherwise,

$$\begin{aligned} x \in \bigcap_{\alpha\in I} Y_\alpha^{\leftarrow} &\Leftrightarrow x \in Y_\alpha^{\leftarrow} \text{ for all } \alpha \in I \\ &\Leftrightarrow xRb \text{ for all } b \in Y_\alpha \text{ for all } \alpha \in I \\ &\Leftrightarrow xRb \text{ for all } b \in \bigcup_{\alpha\in I} Y_\alpha \\ &\Leftrightarrow x \in \left(\bigcup_{\alpha\in I} Y_\alpha\right)^{\leftarrow} \end{aligned}$$

Therefore, $\bigcap_{\alpha\in I} Y_\alpha^{\leftarrow} = \left(\bigcup_{\alpha\in I} Y_\alpha\right)^{\leftarrow}$, and so is closed.

Similarly, let $\{X_\alpha \mid \alpha \in I\}$ be a family of subsets of $A$ for some indexing set $I$. If $\bigcap_{\alpha\in I} X_\alpha^{\rightarrow}$ is empty, then the claim holds trivially, as

$$\bigcap_{\alpha\in I} X_\alpha^{\rightarrow} = \emptyset^{\rightarrow}.$$

Otherwise,

$$\begin{aligned} y \in \bigcap_{\alpha\in I} X_\alpha^{\rightarrow} &\Leftrightarrow y \in X_\alpha^{\rightarrow} \text{ for all } \alpha \in I \\ &\Leftrightarrow aRy \text{ for all } a \in X_\alpha \text{ for all } \alpha \in I \\ &\Leftrightarrow aRy \text{ for all } a \in \bigcup_{\alpha\in I} X_\alpha \\ &\Leftrightarrow y \in \left(\bigcup_{\alpha\in I} X_\alpha\right)^{\rightarrow} \end{aligned}$$

Therefore, $\bigcap_{\alpha\in I} X_\alpha^{\rightarrow} = \left(\bigcup_{\alpha\in I} X_\alpha\right)^{\rightarrow}$, and so is closed. □

Problem 4

Let $A = B = \{q \mid 0 < q < 1 \text{ and } q \text{ is rational}\}$. Let $R$ be the binary operation $\leq$. Identify the system of closed sets. How are they ordered with respect to inclusion?

*Proof.* Let $X \subseteq A$. Since $R$ is $\leq$,

$$X^{\rightarrow} = \{b \mid x \leq b \text{ for all } x \in X\}.$$

Hence, $X^{\rightarrow}$ is the set of all upper bounds of $X$. By definition, $\sup X$ is the least upper bound of $X$, so we can describe the set of all upper bounds of $X$ by

$$X^{\rightarrow} = \{b \in B \mid \sup X \leq b\}.$$

Observe further that, for any $a \in A$, the set $X = \{a\}$ has the property that $\sup X = a$. Additionally, the set $X = \{1 - \frac{1}{n} \mid n \in \mathbb{N}\}$ has $\sup X = 1$, while no subset $X$ of $A$ has $\sup X = 0$. Therefore, the class of closed sets of the form $X^{\rightarrow}$ is precisely

$$\{(a, 1) \cap \mathbb{Q} \mid a \in (0, 1)\} \cup \emptyset$$

Similarly, let $Y \subseteq B$. Since $R$ is $\leq$,

$$Y^{\leftarrow} = \{a \mid a \leq y \text{ for all } y \in Y\}.$$

Hence, $Y^{\leftarrow}$ is the set of all lower bounds of $Y$. By definition, $\inf Y$ is the greatest lower bound of $Y$, so we can describe the set of all lower bounds of $Y$ by

$$Y^{\leftarrow} = \{a \in A \mid a \leq \inf Y\}.$$

Observe further that, for any $b \in B$, the set $Y = \{b\}$ has the property that $\inf Y = b$. Additionally, the set $Y = \{\frac{1}{n} \mid n \in \mathbb{N}\}$ has $\inf Y = 0$, while no subset $Y$ of $B$ has $\inf Y = 1$. Therefore, the class of closed sets of the form $Y^{\leftarrow}$ is precisely

$$\{(0, b) \cap \mathbb{Q} \mid b \in (0, 1)\} \cup \emptyset$$

□

# 1 Problem 5

**Proposition 1.1.** *Let **E** and **F** be fields. **E** is an algebraic closure of **F** if and only if **E** is an algebraic extension of **F** and, for every algebraic extension **K** of **F**, there is an embedding of **K** into **E** that fixes each element of **F**.*

*Proof.* ($\Rightarrow$) Suppose that $\mathbf{E}$ is an algebraic closure of $\mathbf{F}$. Let $\mathbf{K}$ be any algebraic extension of $\mathbf{F}$. We know that $\mathbf{K}$ itself has an algebraically closed extension (call it $\overline{\mathbf{K}}$). Now, $\overline{\mathbf{K}}$ is also an algebraic extension of $\mathbf{F}$ that is algebraically closed, and so $\overline{\mathbf{K}}$ is an algebraic closure of $\mathbf{F}$. By the uniqueness of algebraic closures, we have that $\mathbf{E} \cong \overline{\mathbf{K}}$.

Next, we seek an embedding of $\mathbf{K}$ into $\mathbf{E}$ that fixes each element of $\mathbf{F}$. To this end, define the functions

$$f : \mathbf{K} \to \overline{\mathbf{K}} \text{ the natural embedding of } \mathbf{K} \text{ into } \overline{\mathbf{K}}; \text{ and}$$
$$\phi : \overline{\mathbf{K}} \to \mathbf{E} \text{ the isomorphism between } \overline{\mathbf{K}} \text{ and } \mathbf{E}.$$

The monomorphism $f$ fixes $\mathbf{K}$ (and so fixes $\mathbf{F}$) in $\overline{\mathbf{K}}$ and the isomorphism identifies isomorphic copies of $\mathbf{F}$ in $\overline{\mathbf{K}}$ and $\mathbf{E}$. Therefore, the function $\phi \circ f$ is the desired embedding of $\mathbf{K}$ into $\mathbf{E}$.

($\Leftarrow$) Suppose that $\mathbf{E}$ is an algebraic extension of $\mathbf{F}$ and, for every algebraic extension $\mathbf{K}$ of $\mathbf{F}$, there is an embedding of $\mathbf{K}$ into $\mathbf{E}$ that fixes each element of $\mathbf{F}$. In particular, take $\mathbf{K}$ to be the splitting field of $\mathbf{F}$. By hypothesis, there is an embedding of $\mathbf{K}$ into $\mathbf{E}$ that fixes $\mathbf{F}$. Identifying $\mathbf{K}$ with its isomorphic copy in $\mathbf{E}$, we

see that every polynomial in $\mathbf{F}[x]$ splits in $\mathbf{E}$ (since it splits in $\mathbf{K}$), and so $\mathbf{E}$ is in fact an algebraic closure of $\mathbf{F}$. □

# 2 Problem 6

**Proposition 2.1.** *Let $\boldsymbol{E}$ and $\boldsymbol{F}$ be fields. If $\boldsymbol{E}$ extends $\boldsymbol{F}$ and $[\boldsymbol{E} : \boldsymbol{F}] = 2$, then $\boldsymbol{E}$ is a normal extension of $\boldsymbol{F}$.*

*Proof.* Let $f(x) \in \mathbf{F}[x]$ be irreducible over $\mathbf{F}[x]$ with a root $\alpha \in \mathbf{E}$. Denote the minimal polynomial of $\alpha$ over $\mathbf{F}$ by $\mu_\alpha(x)$. We know that

$$\begin{aligned} \alpha \text{ is a root of } f(x) &\Rightarrow \mu_\alpha(x) \text{ divides } f(x) \\ &\Rightarrow \mu_\alpha(x) = f(x) \qquad \text{(since } f(x) \text{ is irreducible over } \mathbf{F}[x]\text{).} \end{aligned}$$

Now, since $[\mathbf{E} : \mathbf{F}] = 2$, the degree of $\mu_\alpha(x)$ is 2, and so the degree of $f(x)$ 2. As $\alpha$ is a root of $f(x)$, one of its factors is $x - \alpha$, and so $f(x) = (x - \alpha)(x - r)$, for some $r \in \mathbf{F}$ (since $\alpha \cdot r \in \mathbf{F}$). Therefore, $f(x)$ splits over $\mathbf{E}$, as desired. □

# 3 Problem 7

**Proposition 3.1.** *Let $\boldsymbol{E}$ be a field extending the field $\boldsymbol{F}$. Let $\boldsymbol{L}$ and $\boldsymbol{M}$ be intermediate fields such that $\boldsymbol{L}$ is the splitting field of a separable polynomial in $\boldsymbol{F}[x]$. Let $\boldsymbol{L} \vee \boldsymbol{M}$ denote the smallest subfield of $\boldsymbol{E}$ that extends both $\boldsymbol{L}$ and $\boldsymbol{M}$. Under all these conditions, $\boldsymbol{L} \vee \boldsymbol{M}$ is a finite, normal, separable extension of $\boldsymbol{M}$ and $Aut_{\boldsymbol{M}}(\boldsymbol{L} \vee \boldsymbol{M}) \cong Aut_{\boldsymbol{M} \cap \boldsymbol{L}}\boldsymbol{L}$.*

*Proof.* We first show that $\mathbf{L} \vee \mathbf{M}$ is the splitting field of a separable polynomial from $\mathbf{M}[x]$ and then invoke the Key Theorem, which states that this is equivalent to being a finite, normal, separable extension of $\mathbf{M}$.

**Claim 1.** $\mathbf{L} \vee \mathbf{M} = \mathbf{M}[r_0, \ldots, r_{n-1}]$

*Proof.* ($\subset$) As $\mathbf{L} \vee \mathbf{M}$ is the *smallest* subfield of $\mathbf{E}$ that extends both $\mathbf{L}$ and $\mathbf{M}$, it will certainly be contained in $\mathbf{M}[r_0, \ldots, r_{n-1}]$ if $\mathbf{M}[r_0, \ldots, r_{n-1}]$ is indeed an extension of both $\mathbf{L}$ and $\mathbf{M}$. It is evidently an extension of $\mathbf{M}$, and we see that it is also an extension of $\mathbf{L}$ since

$$\begin{aligned} \mathbf{L} &= \mathbf{F}[r_0, \ldots, r_{n-1}] \\ &\subset \mathbf{M}[r_0, \ldots, r_{n-1}] \qquad \text{(since } \mathbf{M} \text{ is an extension of } \mathbf{F}\text{).} \end{aligned}$$

($\supset$) Let $a \in \mathbf{M}[r_0, \ldots, r_{n-1}]$. We see that

$$a = c + \sum_{i=0}^{n-1} c_i r_i \qquad\qquad c, c_i \in \mathbf{M}.$$

Observe also that, since $\mathbf{L} = \mathbf{F}[r_0, \ldots, r_{n-1}]$, the $r_i$ all belong to $\mathbf{L}$ for all $i$. As $\mathbf{L} \vee \mathbf{M}$ is an extension of both $\mathbf{L}$ and $\mathbf{M}$, it follows that $c, c_i$, and $r_i$ belong to $\mathbf{L} \vee \mathbf{M}$ for all $i$. Hence, the linear combination $a$ belongs to $\mathbf{L} \vee \mathbf{M}$, as desired. □

By the above, we conclude that $\mathbf{L} \vee \mathbf{M}$ is a finite, separable, normal extension of $\mathbf{M}$.
Next, define the function

$$\begin{aligned} &\phi : \mathrm{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M}) \to \mathrm{Aut}_{\mathbf{F}}\mathbf{L} \\ &\phi(\sigma) = \sigma \mid_{\mathbf{L}} . \end{aligned}$$

We show that $\phi$ has trivial kernel and that its image is $\mathrm{Aut}_{\mathbf{M} \cap \mathbf{L}}\mathbf{L}$. Given these facts, the Homomorphism Theorem will allow us to conclue that $\mathrm{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M}) \cong \mathrm{Aut}_{\mathbf{M} \cap \mathbf{L}}\mathbf{L}$.

**Claim 2.** The kernel of $\phi$ is trivial.

*Proof.*

$$\begin{aligned}\sigma \in \ker \phi &\Rightarrow \phi(\sigma) = \mathrm{id} \mid_{\mathbf{L}} \\ &\Rightarrow \sigma \mid_{\mathbf{L}} = \mathrm{id} \mid_{\mathbf{L}}\end{aligned}$$

Hence, $\sigma$ fixes all elements of $\mathbf{L}$. As $\sigma \in \mathrm{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M})$, $\sigma$ also fixes all elements of $\mathbf{M}$, and so $\sigma$ fixes $\mathbf{M}[r_0, \ldots, r_{n-1}] = \mathbf{L} \vee \mathbf{M}$. Hence, $\sigma$ is the identity on its domain, and so the kernel of $\phi$ is trivial. □

**Claim 3.** $\mathrm{Inv}(\mathrm{im}\phi) = \mathbf{L} \cap \mathbf{M}$

*Proof.* Let $H = \mathrm{im}\phi$ and $K = \mathrm{Inv}H$. We have that

$$\begin{aligned}H &\leq \mathrm{Aut}_{\mathbf{F}}\mathbf{L} \\ &= \mathrm{Gal}\left(\mathbf{L}/\mathbf{F}\right).\end{aligned}$$

Since $H$ is finite, the Key Theorem implies that

$$H = \mathrm{Aut}_{\mathbf{K}}\mathbf{L}.$$

Hence, it suffices to show that $\mathbf{K} = \mathbf{L} \cap \mathbf{M}$. To that end, let $a \in \mathbf{L} \cap \mathbf{M}$. Observe that

$$\begin{aligned}\phi(\sigma)(a) &= \sigma \mid_{\mathbf{L}} (a) \\ &= a \qquad\qquad (\text{since } a \in M).\end{aligned}$$

Hence, $\mathbf{L} \cap \mathbf{M} \subset \mathbf{K}$.

For the reverse inclusion, let $a \in \mathbf{K}$. As before,

$$\begin{aligned}\phi(\sigma)(a) &= \sigma \mid_{\mathbf{L}} (a) \\ &= a \qquad\qquad (\text{since } a \in K),\end{aligned}$$

and so $a \in L$. We also have

$$\begin{aligned}\sigma \mid_{\mathbf{L}} (a) &= a \\ \Rightarrow \sigma(a) &= a,\end{aligned}$$

and so $a \in \mathrm{Inv}\left(\mathrm{Aut}\left(\mathbf{L} \vee \mathbf{M}\right)\right)$, but this is just $M$ (by the Key Theorem). Hence, $a \in \mathbf{L} \cap \mathbf{M}$. □

Finally, the Homomorphism Theorem gives that $\mathrm{Aut}_{\mathbf{M}}(\mathbf{L} \vee \mathbf{M}) \cong \mathrm{Aut}_{\mathbf{M} \cap \mathbf{L}}\mathbf{L}$, thus completing the proof. □

# 4 Problem 8

**Proposition 4.1.** *Let $\boldsymbol{L}$ and $\boldsymbol{M}$ be fields. View the collection of functions from $\boldsymbol{L}$ into $\boldsymbol{M}$ as a vector space over $\boldsymbol{M}$ with addition defined in the usual way. The collection of field embeddings from $\boldsymbol{L}$ into $\boldsymbol{M}$ is a linearly independent set in this vector space.*

*Proof.* Suppose, for the purpose of contradiction, that the collection of field embeddings from $\mathbf{L}$ into $\mathbf{M}$ is not linearly independent set. Choose minimal $k$ such that

$$c_0\phi_0 + \cdots + c_k\phi_k = 0 \qquad\qquad c_i \in \mathbf{M},\ \phi_i \text{ field embeddings from } \mathbf{L} \text{ into } \mathbf{M}$$

with $c_i \neq 0$ for all $i$. Without loss of generality, there exists $x'$ such that $\phi_0(x') \neq \phi_1(x')$ and further that $\phi_0(x') \neq 0$. It follows that

$$\begin{aligned}0 &= \phi_0(x')(c_0\phi_0 + \cdots + c_k\phi_k) \\ &= c_0\phi_0(x')\phi_0 + \cdots + c_k\phi_0(x')\phi_k.\end{aligned}$$

Consider the evaluation at $xx'$.

$$\begin{aligned} 0 &= c_0\phi_0(xx') + \cdots + c_k\phi_k(xx') \\ &= c_0\phi_0(x)\phi_0(x') + \cdots + c_k\phi_k(x)\phi_k(x') \end{aligned}$$

Hence,

$$\begin{aligned} 0 &= (c_0\phi_0(x')\phi_0 + \cdots + c_k\phi_0(x')\phi_k) - (c_0\phi_0(x)\phi_0(x') + \cdots + c_k\phi_k(x)\phi_k(x')) \\ &= c_1(\phi_0(x') - \phi_1(x'))\phi_1(x) + \cdots + c_k(\phi_0(x') - \phi_k(x'))\phi_k(x), \end{aligned}$$

which is a shorter nontrivial linear combination, contradiction the minimality of $k$. Therefore, we conclude that the collection of field embeddings from $\mathbf{L}$ into $\mathbf{M}$ is indeed a linearly independent set in this vector space. □

# 5 Problem 9

**Proposition 5.1.** *Let $\boldsymbol{F}$ be a field. We use $\boldsymbol{F}^\times$ to denote the group of nonzero elements of $\boldsymbol{F}$ under multiplication and the formation of multiplicative inverses. Every finite subgroup of $\boldsymbol{F}^\times$ is a cyclic group.*

*Proof.* Let $\mathbf{G}$ be a finite subgroup of $\mathbf{F}^\times$. Since $\mathbf{F}$ is a field, we know that $\mathbf{G}$ is Abelian. By the Fundamental Theorem of Finite Abelian Groups, $\mathbf{G} \cong \mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_k}^{n_k}$ where the $p_i$ are distinct primes and the $n_i$ are positive integers.

If $n_i = 1$ for all $i$, the Chinese Remainder Theorem gives that the element $(1, \ldots, 1)$ generates $\mathbf{G}$ (as the $p_i$ are relatively prime), and so $\mathbf{G}$ is cyclic.

Suppose now, for the purpose of contradiction, that $n_j \geq 2$ for some $j$, then $\mathbf{G}$ has $\mathbb{Z}_{p_j} \times \mathbb{Z}_{p_j}$ as a subgroup. For any $a, b \in \mathbb{Z}_{p_j}$, Lagrange's Theorem gives that $(a, b)^{p_j} = 1$. In other words, there are $p_j^2$ roots of $x^{p_j} - 1$, which is a contradiction. Hence, $n_i = 1$ for all $i$, and so $\mathbf{G}$ is cyclic by the previous argument. □

# 6 Problem 10

**Proposition 6.1.** *Let $p$ be a prime and let $H$ be a subgroups of $S_p$. If $H$ has a transposition and an element of order $p$, then $H = S_p$.*

*Proof.* Let $a, b \in H$ with $a$ of order $p$ and $b$ a transposition. Without loss of generality, let $b = (0\ 1)$. As $a$ has order $p$ and $p$ is prime $p$, we have that $a$ is $p$-cycle. Therefore, $a^k = (0\ 1 \ldots)$ for some $k$. We can re-index the other elements so that we have $a^k = (0\ 1 \ldots p{-}1)$. Let $c = a^k$. Then $cbc^{-1} = (0\ 1 \ldots p{-}1)(0\ 1)(p{-}1 \ldots 0\ 1) = (0)(1\ 2)(3)...(p-1) = (1\ 2)$. By induction, we have $c^k b c^{-k} = c(c^{k-1}bc^{-k+1})c^{-1} = (k+1\ \ k+2)$. Therefore, we have that $(0\ 1), (1\ 2), ..., (p-2\ \ p-1)$ are generated by $\{a, b\}$. Let $(xy)$ be a transposition. Then $(x\ \ x+1)(x+1\ \ x+2)\cdots(y-1\ \ y) = (x\ \ y)$ and $(x\ \ y)$ is also generated by $\{a, b\}$. As every permutation can be decomposed into transpositions we conclude that $\{a, b\}$ generates $S_p$. □

# 7 Problem 11

**Proposition 7.1.** *The polynomial $f(x) = x^5 - 2x^3 - 8x + 2$ is not solvable by radicals over the field of rational numbers.*

*Proof.* Observe first that, by Eisenstein's Criterion, $f(x)$ is irreducible over $\mathbb{Q}$. Next, notice that

$$\begin{aligned} f'(x) &= 5x^4 - 6x^2 - 8 \\ &= (5x^2 + 4)(x^2 - 2). \end{aligned}$$

Let $a_0, a_1$, and $a_2$ be the distinct real roots of $f(x)$. We also have complex roots $a_3$ and $a_4$ with $a_3 = \overline{a_4}$. Let $E$ be the splitting field over $\mathbb{Q}$ of $f(x)$. It must be that $\mathrm{Gal}(E/\mathbb{Q})$ contains a 2-cycle (there is an automorphism transposing $a_3$ and $a_4$ but fixing every other element). We also have that $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$, which implies that $5 \mid [E : \mathbb{Q}]$. This in turn gives that $\mathrm{Gal}(E/\mathbb{Q})$ conains an element of order 5. By problem 10 above, we have that $Gal(E/\mathbb{Q}) \cong S_5$, which is no solvable. Hence, $f(x)$ is not solvable by radicals. □

# 8 Problem 12

**Proposition 8.1.** *Let $F$ be a finite field. The product of all the nonzero elements of $F$ is equal to -1.*

*Proof.* Let $|F| = p^k$. Evidently, $|F^\times| = p^k - 1$. Furthermore, $F^\times$ is cyclic (and so abelian). Let $\sigma$ be a generator for $F^\times$. We have that $\sigma^{p^k-1} = 1$ and $\sigma^m \neq 1$ for $m < p^k - 1$.

Suppose $p = 2$. For any $k$, $2^k - 1$ is odd. Here, the only self-inverse element is 1, so the product $1 \cdot \sigma \cdot \cdots \cdot \sigma^{2^k-2}$ can be arranged such that inverse pairs are group together. Hence, the product is equal to 1, which is congruent to -1 modulo 2.

Suppose $p$ is an odd prime. For any $k$, $p^k - 1$ is even. Here, the self-inverse elements are 1 and $\sigma^{\frac{p^k-1}{2}}$, so the product $1 \cdot \sigma \cdot \cdots \cdot \sigma^{p^k-2}$ can be arranged such that inverse pairs are group together. Hence, the product is equal to $\sigma^{p^k-2}$, which is congruent to -1 modulo p. □

**Corollary 8.2.** *(Wilson's Theorem) For every prime number $p$, $(p-1)! \equiv -1$ (mod $p$).*

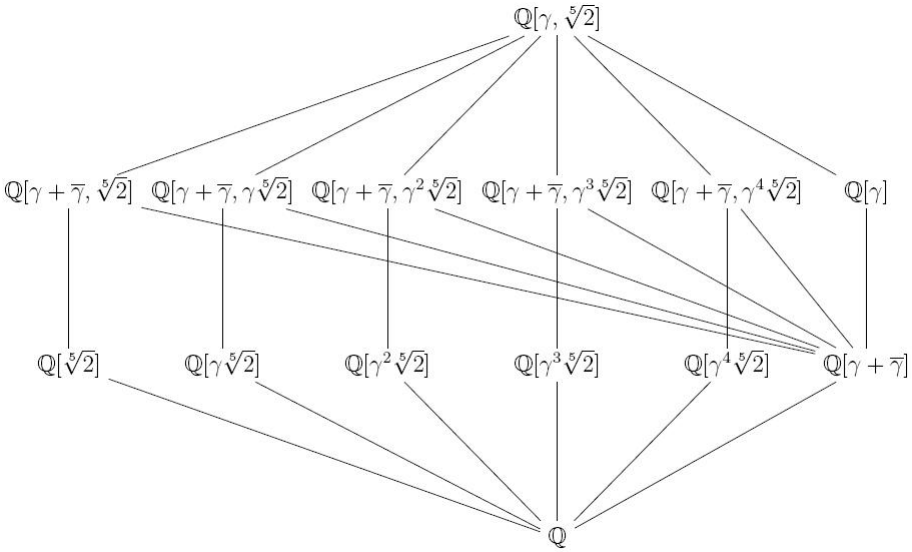
*Proof.* The elements of $F_p^\times$ are precisely $1, \ldots, p-1$, and so by the proposition above gives

$$\begin{aligned}(p-1)! &= 1 \cdot \cdots \cdot (p-1) \\ &= -1 \text{ (in } F_p^\times).\end{aligned}$$

In other words, $(p-1)! \equiv -1 \pmod{p}$. □

# 9 Problem 13

Let $E$ be the splitting field of $x^5 - 2$ over $\mathbb{Q}$. The lattice of all fields intermediate between $\mathbb{Q}$ and $E$ is pictured below, where $\gamma$ represents a primitive fifth root of unity.




(Many thanks to K. Brown for the image.)

# 10 Problem 14

Let $F$ be a field of prime characteristic $p$. Let $E$ be a field extending $F$. The field $E$ is a normal separable extension of $F$ of dimension $p$ if and only if $E$ is the splitting field over $F$ of an irreducible polynomial of the form $x^p - x - a$ for some $a \in F$.

*Proof.* ($\Rightarrow$) Let $E$ be a normal, separable extension of $F$ having dimension $p$. We have that $|\mathrm{Gal}(E/F)| = p$, and so $\mathrm{Gal}(E/F)$ is cyclic. Let $\sigma$ generate $\mathrm{Gal}(E/F)$. The automorphisms of $E$ are $1, \sigma, \sigma^2, \ldots, \sigma^{p-1}$. Define

$$t = 1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1}.$$

We know that these automorphisms are linearly independent, so there is $v \in E$ such that

$$t(v) = v + \sigma(v) + \sigma^2(v) + \cdots + \sigma^{p-1}(v) = u \neq 0.$$

Apply $\sigma$ to $u$ to get

$$\begin{aligned}\sigma(u) &= \sigma(v) + \sigma^2(v) + \sigma^3(v) + \cdots + \sigma^{p-1}(v) + \sigma^p(v) \\ &= 1 + \sigma(v) + \sigma^2(v) + \cdots + \sigma^{p-1}(v).\end{aligned}$$

Hence, $\sigma(u) = u$. As $u$ is fixed by $\sigma$, it must be that $u \in F$, and so $v \in (E \setminus F)$. Let now $v' = vu^{-1}$. We have that $t(v') = 1$, so assume (without loss of generality) that $t(v) = 1$.

Let

$$w = v + 2\sigma(v) + 3\sigma^2(v) + \cdots + (p-1)\sigma^{p-2}(v).$$

We have that

$$\begin{aligned}w - \sigma(w) &= v + 2\sigma(v) + 3\sigma^2(v) + \cdots + (p-1)\sigma^{p-2}(v) \\ &\quad - \big(\sigma(v) + 2\sigma^2(v) + 3\sigma^3(v) + \cdots + (p-1)\sigma^{p-1}(v)\big) \\ &= v + \sigma(v) + \sigma^2(v) + \cdots + \sigma^{p-1}(v) \\ &= 1.\end{aligned}$$

Hence, $\sigma(w) = w - 1$. Now, let $\gamma = -w$ to obtain

$$\sigma(\gamma) = \sigma(-w) = -\sigma(w) = -(w-1) = -w + 1 = \gamma + 1.$$

This entails that $\gamma = -w \in (E \setminus F)$, and so $F[\gamma]$ has dimension $p$ over $F$. As $\sigma(\gamma^p) = \sigma(\gamma)^p = (\gamma+1)^p = \gamma^p + 1$, we have that

$$\sigma(\gamma^p - \gamma) = (\gamma+1)^p - (\gamma+1) = \gamma^p - \gamma.$$

Hence, $\gamma^p - \gamma \in F$. Let now $a = \gamma^p - \gamma$. We see that $x^p - x - a$ has roots $\gamma, \gamma+1, \gamma+2, \ldots, \gamma+(p-1)$, and so $E$ is the splitting field of $f(x) = x^p - x - a$.

($\Leftarrow$) Let $E$ be the splitting field over $F$ of the irreducible polynomial $f(x) = x^p - x - a$. As $f'(x) = -1$, we have that $f(x)$ and $f'(x)$ share no common roots, and so $f(x)$ is separable. Now, let $u \in E$ be a root of $f(x)$. It follows that

$$\begin{aligned}f(u+1) &= (u+1)^p - (u+1) - a \\ &= u^p + 1^p - u - 1 - a \\ &= u^p - u - a \\ &= 0.\end{aligned}$$

Hence, $u+1$ is also a root of $f(x)$. Proceeding inductively, $u, u+1, u+2, \ldots, u+(p-1)$ are the $p$ distinct roots of $f(x)$. Hence, $E$ is a normal separable extension of $F$ of dimension $p$. □

# 11 Problem 17

**Proposition 11.1.** *Let $R$ be a real closed field and let $f(x) \in R[x]$. Suppose that $a < b$ in $R$ and that $f(a)f(b) < 0$. There is $c \in R$ with $a < c < b$ such that $c$ is a root of $f(x)$.*

*Proof.* Assume $f(x)$ is monic, and so $f(x) = (x-r_0)(x-r_1)\cdots(x-r_m)g_1(x)\cdots g_s(x)$ with $g_i(x) = x^2+c_ix+d_i$ and $c_i^2 < 4d_i$. It follows that

$$\begin{aligned} g_i(x) &= \left(x + \frac{c_i}{2}\right)^2 + \frac{1}{4}(4d_i - c_i^2) \\ &= \left(x + \frac{c_i}{2}\right)^2 + e_i^2, \end{aligned}$$

where $e_i^2 = \frac{1}{2}\sqrt{4d_i - c_i^2}$. Now, $g_i(u) > 0$ for all $u \in R$. If $a < r_i$ and $b < r_i$ for all $1 \leq i \leq m$, then $f(a)f(b) = (a-r_i)(b-r_i)g_j(a)g_j(b) > 0$. Similarly, if $a > r_i$ and $b > r_i$ for all $1 \leq i \leq m$, then $f(a)f(b) > 0$. Since $f(a)f(b) < 0$, it follows that either $a < r_j < b$ or $b < r_j < a$ for some $1 \leq j \leq m$. As $r_j$ is a root of $f$, we take $r_j$ to be $c$. □

# 12 Problem 18

**Proposition 12.1.** *Let $R$ be a real closed field, let $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n = f(x) \in R[x]$, and put $M = |a_0| + |a_1| + \cdots + |a_{n-1}| + 1$. Every root of $f(x)$ that belongs to $R$ belongs to the interval $[-M, M]$.*

*Proof.* Let $r$ be any root of $f$. Since $|M| \geq 1$, we can assume $|r| > 1$ (otherwise, we are already finished). Now,

$$\begin{aligned} f(r) &= a_0 + a_1r + \cdots + a_{n-1}r^{n-1} + r^n \\ &= r^n\left(\frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} + 1\right). \end{aligned}$$

As $r$ is a root $f$,

$$\begin{aligned} 0 &= r^n\left(\frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} + 1\right) \\ 0 &= \frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} + 1 \\ -1 &= \frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} \\ 1 &= \left|\frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r}\right| \\ 1 &\leq \left|\frac{a_0}{r^n}\right| + \left|\frac{a_1}{r^{n-1}}\right| + \cdots + \left|\frac{a_{n-1}}{r}\right| \\ 1 &\leq \left|\frac{a_0}{r}\right| + \left|\frac{a_1}{r}\right| + \cdots + \left|\frac{a_{n-1}}{r}\right| \\ |r| &\leq |a_0| + |a_1| + \cdots + |a_{n-1}| \\ |r| &\leq M, \end{aligned}$$

as desired. □

# 13 Problem 19

**Proposition 13.1.** *Every element of a finite field can be written as the sum of two squares.*

*Proof.* Let $F$ be a finite field having characteristic $p$ and $|F| = p^n$. Define $\phi : F \to F$ by $\phi(x) = x^2$. If $p = 2$, then $\phi$ is an isomorphism, and so for any $u \in F$ there is $v \in F$ with $u = v^2 + 0^2$. If $p > 2$, then for all $x, y \in F$, $x^2 = y^2$ implies that $(x+y)(x-y) = 0$. Hence, $y = x$ or $y = -x$, and so $|Im\phi| \geq \frac{p^n+1}{2}$. Let $m = \frac{p^n+1}{2}$ and choose distinct elements $x_1^2, \ldots, x_m^2$ in $F$. Hence, for any $u \in F$ and for all $1 \leq i \leq m$, $u - x_i^2$ are distinct elements in $F$. Since $2m > p^n$, there exists $j$ and $k$ such that $x_j^2 = u - x_k$. That is, $u = x_j^2 + x_k^2$, as desired. □

# 14 Problem 20

**Proposition 14.1.** *Every polynomial with rational coefficients that has a splitting field of dimension 1225 over the rationals is solvable by radicals.*

*Proof.* Let $E$ be a splitting field of dimension 1225 over the rationals. A polynomial with rational coefficients is solvable by radicals if and only if $\text{Gal}(E/\mathbb{Q})$ is solvable. We argue that $\text{Gal}(E/\mathbb{Q})$ is Abelian, and hence solvable, as every Abelian group is solvable.

Let $G = \text{Gal}(E/\mathbb{Q})$. Observe first that $1225 = 5^2 7^2$. Consider the Sylow $p$-subgroups of $G$. Sylow's theorem gives

- $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 49$, so $n_5 = 1$
- $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 25$, so $n_7 = 1$

Hence, $\mathbf{G}$ has a unique Sylow 5-subgroup $\mathbf{N}_5$ and a unique Sylow 7-subgroup $\mathbf{N}_7$. The uniqueness of each of these groups implies that they are normal in $\mathbf{G}$.

Observe next that $\mathbf{N}_5 \cap \mathbf{N}_7$ is trivial, since only the identity element can have order dividing both $|\mathbf{N}_5|$ and $|\mathbf{N}_7|$. By the Third Isomorphism theorem, we have

$$\mathbf{N}_5\mathbf{N}_7/\mathbf{N}_7 \cong \mathbf{N}_5/\mathbf{N}_5 \cap \mathbf{N}_7 = \mathbf{N}_5$$

Applying Lagrange's theorem, we have

$$\begin{aligned} \left|\mathbf{N}_5\mathbf{N}_7/\mathbf{N}_7\right| &= |\mathbf{N}_5| \\ \frac{|\mathbf{N}_5\mathbf{N}_7|}{|\mathbf{N}_7|} &= |\mathbf{N}_5| \\ |\mathbf{N}_5\mathbf{N}_7| &= |\mathbf{N}_5||\mathbf{N}_7| = |\mathbf{G}| \end{aligned}$$

Hence, $\mathbf{G} \cong \mathbf{N}_5 \times \mathbf{N}_7$.

We proceed by showing $\mathbf{N}_5$ is Abelian. Since $\mathbf{N}_5$ is of prime power order, it has a nontrivial center $Z(\mathbf{N}_5)$. Furthermore, $Z(\mathbf{N}_5)$ is normal in $\mathbf{N}_5$, so $\mathbf{N}_5/Z(\mathbf{N}_5)$ is a group of size 1 or 5. If it is of size 5, then it is cyclic. We claim that this is impossible in general.

**Claim 4.** If a group $\mathbf{G}$ properly contains its center, then $\mathbf{G}/Z(\mathbf{G})$ is not cyclic.

*Proof.* Suppose, to the contrary, that $\mathbf{G}/Z(\mathbf{G})$ is cyclic generated by $aZ(\mathbf{G})$. We argue that $G$ is Abelian. Let $b$ and $c$ be elements of $G$. We can find integers $m$ and $n$ so that

$$\begin{aligned} bZ(\mathbf{G}) &= a^m Z(\mathbf{G}) \\ cZ(\mathbf{G}) &= a^n Z(\mathbf{G}) \end{aligned}$$

This further implies that we can find elements $d$ and $e$ in $Z(\mathbf{G})$ so that

$$\begin{aligned} b &= a^m d \\ c &= a^n e \end{aligned}$$

Observe that $d$ and $e$ commute freely with any element since they are in the center. Furthermore, powers of $a$ commute with each other. It follows that

$$\begin{aligned} bc &= (a^m d)(a^n e) \\ &= (a^n e)(a^m d) \\ &= cb \end{aligned}$$

Hence, $\mathbf{G}$ is Abelian, so $Z(\mathbf{G}) = \mathbf{G}$, which contradicts our assumption that $\mathbf{G}$ properly contains its center. Therefore, we conclude that $\mathbf{G}/Z(\mathbf{G})$ is not cyclic. □

Citing the claim above, we conclude that $\mathbf{N}_5/Z(\mathbf{N}_5)$ is of size 1. In other words, $\mathbf{N}_5$ is Abelian.

Similarly, we can show that $\mathbf{N}_7$ is Abelian (replace every occurrence of "5" with "7" in the argument for $\mathbf{N}_5$).

Taken together, we see that $\mathrm{Gal}(E/\mathbb{Q})$ is Abelian, and so is solvable. □

# 15 Problem 21

**Proposition 15.1.** *Let $F$ be a field. The following are equivalent.*

1. *$F$ is not algebraically closed, but there is a finite upper bound on the degrees of the irreducible polynomials in $F[x]$.*
2. *$F$ is a real closed field.*

*Proof.* $(1 \Rightarrow 2)$ We claim first that if there is an upper bound for the degrees of the irreducible polynomials in $F[x]$, then $F$ is perfect. If not, then $F$ has characteristic $p \neq 0$ and some $a \in F$ is not a $p^{\text{th}}$ power in $F$. We have shown that $f(x) = x^{p^t} - c$ is irreducible for every $t \geq 0$, which is a contradiction with the fact that there is a finite upper bound on the degrees of the irreducible polynomials in $F[x]$. Hence, $F$ is perfect. Let $K$ be the algebraic closure of $F$. Now, we also have that $K$ is separable over $F$, so the degree of every element of $K$ over $F$ is bounded. Therefore, $[K : F]$ is finite, and so $F$ is real closed by the Artin-Schreir Theorem.

$(2 \Rightarrow 1)$ Let $K$ denote the algebraic closure of $F$. Since $F$ is real closed, $K = F[\sqrt{-1}]$, and so $[K : F] = 2$. Hence, every irreducible polynomial in $F[x]$ is at most quadratic. □

# 16 Problem 22

Let $E$ be the splitting field over $\mathbb{Q}$ of $x^4 - 2$. We determine the lattice of intermediate fields between $E$ and $\mathbb{Q}$.

Observe first that $x^4 - 2 = (x + \sqrt[4]{2})(x - \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})$, and so $E = \mathbb{Q}[i, \sqrt[4]{2}]$. Now, the elements of the Galois group are determined by their action on the roots of $x^4 - 2$ and, furthermore, their action is restricted to permutations of these roots. Finally, if $\phi$ is an element of the Galois group $\phi(-\sqrt[4]{2}) = -\phi(\sqrt[4]{2})$ and $\phi(-i) = -\phi(i)$. Hence, we can determine the permutations by sending $\sqrt[4]{2}$ to any of the four roots (which also determines the action on $-\sqrt[4]{2}$) and then sending $i$ to any of the remaining two roots (which also determine the action on $-i$), giving a total of 8 distinct permutations. Define

$$\sigma(x) = -x$$

and

$$\tau(x) = \begin{cases} i & : x = \sqrt[4]{2} \\ -i & : x = i \\ -\sqrt[4]{2} & : x = -i \\ \sqrt[4]{2} & : x = -\sqrt[4]{2} \end{cases}.$$

Computation shows that $\{1, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\}$ are the desired permutations, and so the Galois group is isomorphic to $D_8$. We conclude with a presentation of the lattice of subgroups of $D_8$ (which is well-known), and invoke the Fundamental Theorem of Galois Theory which states that the lattice of subfields of $\mathbb{Q}[i, \sqrt[4]{2}]$ is determined by computing the fixed field of each subgroup of $D_8$ (generating a lattice of subfields that is "upside-down isomorphic" to the lattice of subgroups).

## 17 Problem 23

**Proposition 17.1.** *The field of real numbers has only one ordering that makes it into an ordered field.*

*Proof.* Any ordering $\leq$ of $\mathbb{R}$ must admit that if $x \leq y$, then $y - x \geq 0$. Since $\mathbb{R}$ is real closed, every positive element of $\mathbb{R}$ is a square. Hence, we can define the relation $x \leq y$ if and only if $y - x = a^2$ for some $a \in \mathbb{R}$. Since the choice of $a$ (if it exists) is unique for each $x, y \in \mathbb{R}$, there can be only one ordering of $\mathbb{R}$. $\square$