Problem 37.
Let $F$ be the subring of the field of complex numbers consisting of those numbers of the form $a + ib$ where $a$ and $b$ are rational. Let $G$ be the subring of the field of complex numbers consisting of those numbers of the form $m + ni$ where $m$ and $n$ are integers.

(a) Describe all the units of $G$.
(b) Prove that $F$ is (isomorphic to) the field of fractions of $G$.
(c) Prove that $G$ is a principal ideal domain.

[Hint: In this problem it is helpful to consider the function that sends each complex number $z$ to $z \bar{z} = |z|^2$.]

Solution

Let $N(z) = z \bar{z} = |z|^2$. This makes sense for any complex number. Notice $N(a + bi) = a^2 + b^2$ when $a$ and $b$ are real numbers. In particular, if $z \in G$, then $N(z)$ is a natural number. It is easy to check that $N(zw) = N(z)N(w)$, which is why the function $N$ is useful to us here.

For part (a), suppose $z, w \in G$ and $zw = 1$. Then $N(z)N(w) = N(1) = 1$ and both $N(z)$ and $N(w)$ must be natural numbers. The only natural number that is a factor of 1 is 1 itself. So we see that $N(z) = 1 = N(w)$. This means that $z$ and $w$ must lie on the unit circle in the complex plane. The only member of $G$ with this property are $1, -1, i,$ and $-i$. These are the only possibilities for the units of $G$. Evidently, each of these four is a unit, so we have found them all.

For part (b) we first establish that $F$ is a field. It is straightforward to check that $F$ is closed with respect to addition and multiplication and that $0, 1 \in F$. So $F$ is certainly a subring. We have to show that every nonzero element of $F$ has a multiplicative inverse in $F$. Let $a + bi \in F$ where $a, b \in \mathbb{Q}$ and $a + bi \neq 0$. Notice this means $a - bi \neq 0$ as well. But now observe

$$\frac{1}{a + bi} = \frac{1}{a + bi} \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i.$$  

So the multiplicative inverse in $C$ of $a + bi$ already belongs to $F$. So $F$ is a field. It is evidently the smallest subfield of $C$ that contains $G$. We know from class that such a smallest subfield is isomorphic to the field of fractions of $G$.

For part (c) it helps to see that on the plane $G$ consists of all the points ‘with integer coordinates’. For any complex number $z$ there is usually a member of $G$ closest to $z$. We let $\lfloor z \rfloor$ denote a member of $G$ closest to $z$, favoring the points of $G$ to the left and above $z$ to break any ties. For example $\lfloor \frac{1}{2} + \frac{1}{2}i \rfloor = 1 + i$. For any complex number $z = x + yi$ we see that $\lfloor z \rfloor$ must be one of the following four members of $G$:

$$\lfloor x \rfloor + \lfloor y \rfloor i, \quad \lfloor x \rfloor + \lceil y \rceil i, \quad \lceil x \rceil + \lfloor y \rfloor i, \quad \lceil x \rceil + \lceil y \rceil i.$$  

But notice that $|x - \lfloor x \rfloor| \leq \frac{1}{2}$ for any real number. Similar inequalities hold for $\lfloor x \rfloor$. This means that

$$N(z - \lfloor z \rfloor) \leq \left( \frac{1}{2} \right)^2 + \left( \frac{1}{2} \right)^2 = \frac{1}{2}.$$  

Let $I$ be a nontrivial ideal of $G$.

The set $\{ N(z) \mid z \in I \text{ and } z \neq 0 \}$ is a nonempty set of positive integers. So it has a least element. Pick $z \in I$ with $z \neq 0$ and $N(z)$ as small as possible. We need to
see that if $u \in I$ then $u = zw$ for some $w \in G$. Let us try $w = \lfloor \frac{u}{z} \rfloor$. At least this belongs to $G$. So both $u \in I$ and $\lfloor \frac{u}{z} \rfloor z \in I$. Consequently, $u - \lfloor \frac{u}{z} \rfloor z \in I$. I contend that

$$N \left( u - \lfloor \frac{u}{z} \rfloor z \right) < N(z).$$

Once this is shown, given the minimality of $z$, we see that $N(u - \lfloor \frac{u}{z} \rfloor z) = 0$. This in turn implies that $u = \lfloor \frac{u}{z} \rfloor z$, as desired. Here is how to establish the contention

$$N \left( u - \lfloor \frac{u}{z} \rfloor z \right) = N \left( \left( \frac{u}{z} - \lfloor \frac{u}{z} \rfloor \right) z \right)$$

$$= N \left( \frac{u}{z} - \lfloor \frac{u}{z} \rfloor \right) N(z)$$

$$\leq \frac{1}{2} N(z)$$

$$< N(z)$$

The ring $G$ is called the ring of Gaussian integers.

---

**Problem 38.**
Let $R$ and $S$ be commutative Noetherian rings. Prove that $R \times S$ is also Noetherian.

---

**Solution**
Let $I$ be an ideal of $R \times S$. We will show that $I$ is finitely generated. Suppose that $(a, b) \in I$. Since $(1, 0) \in R \times S$ and $I$ is an ideal, we see that $(a, 0) = (1 \cdot a, 0 \cdot 0) = (1, 0) \cdot (a, b) \in I$. This means that for any $a \in R$ we get $(a, b) \in I$ for some $b \in S$ if and only if $(a, 0) \in I$. Likewise, for any $b \in S$ we get $(a, b) \in I$ for some $a \in R$ if and only if $(0, b) \in I$.

Now let $I_s = \{ a \mid (a, 0) \in I \}$ and let $I^* = \{ b \mid (0, b) \in I \}$. It is straightforward to prove that $I_s$ is an ideal of $R$ and that $I^*$ is an ideal of $S$. Since these two rings are Noetherian we know that both these ideals are finitely generated. Let the elements $a_0, a_1, \ldots, a_n$ generate $I_s$ and let the elements $b_0, b_1, \ldots, b_m$ generate $I^*$. I contend that the finitely many elements

$$(a_0, 0), (a_1, 0), \ldots, (a_n, 0), (0, b_0), (0, b_1), \ldots, (0, b_m)$$

generate the ideal $I$. It is evident that each one of them belongs to $I$. Now let $(u, v)$ be an arbitrary element of $I$. As pointed out above, this means $(u, 0)$ and $(0, v)$ both belong to $I$. Hence $u \in I_s$ and $v \in I^*$. So pick $r_0, \ldots, r_n \in R$ and $s_0, \ldots, s_m \in S$ so that

$$u = r_0 a_0 + \cdots + r_n a_n \quad \quad v = s_0 b_0 + \cdots + s_m b_m.$$ 

From this we get

$$(u, 0) = (r_0, 0)(a_0, 0) + \cdots + (r_n, 0)(a_n, 0) \quad \quad (0, v) = (0, s_0)(0, b_0) + \cdots + (0, s_m)(0, b_m).$$

But then $(u, v) = (u, 0) + (0, v)$ is generated by the elements

$$(a_0, 0), (a_1, 0), \ldots, (a_n, 0), (0, b_0), (0, b_1), \ldots, (0, b_m).$$

So we conclude that these finitely many elements generate $I$. Consequently, $R \times S$ is Noetherian.

---

**Problem 39.**
Let $F$ and $M$ be modules over the same ring and let $F$ be a free module. Let $h : M \to F$ be a homomorphism from $M$ onto $F$. Prove each of the following.
(a) There is an embedding \( g : F \rightarrow M \) of \( F \) into \( M \) such that \( h \circ g = \text{id}_F \). (Here \( \text{id}_F \) denotes the identity map of the set \( F \).)

(b) \( M = \ker h \oplus F' \), where \( F' \) is the image of \( F \) with respect to \( g \).

**Solution**

Let \( B \) be a basis for \( F \). For each \( b \in B \) pick \( m_b \in M \) so that \( h(m_b) = b \). This is possible since \( h \) maps \( M \) onto \( F \). Since \( B \) is a basis for the free module \( F \) there is a unique homomorphism \( g : F \rightarrow M \) such that \( g(b) = m_b \) for each \( b \in B \). Observe that the map \( h \circ g \) is a homomorphism from \( F \) to \( F' \) such that each \( b \in B \) is mapped to itself. By the freeness of \( F \) there is only one such homomorphism. Of course, the identity map of \( F \) has this property. So it must be that \( h \circ g \) is the identity map on \( F \).

This entails that \( g \) must be one-to-one. So \( g \) embeds \( F \) into \( M \). This establishes part (a).

For part (b) we need to show two things: that \( \ker h \cap F' \) is trivial and that every element of \( M \) can be written as the sum of an element of \( \ker h \) and an element of \( F' \). For the first, suppose \( v \in \ker h \cap F' \). Since \( v \in F' \) pick \( u \in F \) so that \( v = g(u) \). Since \( v \in \ker h \), we find

\[
0 = h(v) = h(g(u)) = u
\]

by part (a). Since \( u = 0 \) and \( v = g(u) \), we see that \( v = 0 \). In this way, we find \( \ker h \cap F' \) is trivial. For the second condition in the definition of direct sum, let \( w \in M \). Since \( w = (w - g(h(w))) + g(h(w)) \) and \( g(h(w)) \in F' \), it will be enough for us to show that \( w - g(h(w)) \in \ker h \). So look at

\[
h(w - g(h(w))) = h(w) - h(g(h(w))) = h(w) - h(w) = 0
\]

and \( w - g(h(w)) \in \ker h \), has desired.

---

**Problem 40.**

Let \( M \) and \( N \) by finitely generated modules over the same principal ideal domain. Prove that if \( M \times N \times M \cong N \times M \times N \), then \( M \cong N \).

**Solution**

Let \( R \) denote the principal ideal domain. Let \( d(q, P) \) be the function defined, whenever \( q \) is a positive power of some prime element of \( r \) or when \( q = 0 \) and whenever \( P \) is a finitely generated \( R \)-module, so that \( d(q, P) \) counts the number of directly indecomposable direct factors in any complete direct decomposition of \( P \) which are of order \( q \) (if \( q \) is the power of a prime) or which are free (if \( q = 0 \)). The Structure Theorem for Finitely Generated Modules over of PID ensures that this function \( d \) exists and that finitely generated \( R \)-modules \( P \) and \( P' \) are isomorphic if and only if \( d(q, P) = d(q, P) \) for all values of \( q \).

So be know for all appropriate \( q \)

\[
d(q, M \times N \times M) = d(q, N \times M \times N).
\]

But now consider

\[
d(q, M) = d(q, M) + d(q, N) + d(q, M) - d(q, M) - d(q, N)
= d(q, M \times N \times M) - d(q, M) - d(q, N)
= d(q, N \times M \times N) - d(q, M) - d(q, N)
= d(q, N) + d(q, M) + d(q, N) - d(q, M) - d(q, N)
= d(qN).
\]

So we conclude that \( M \cong N \).
PROBLEM 41.

Give an example of two dissimilar matrices $A$ and $B$ with real entries that have all the following properties:

(a) $A$ and $B$ have the same minimal polynomial,
(b) $A$ and $B$ have the same characteristic polynomial, and
(c) The common minimal polynomial has no real roots.

**Solution**

We know that every square matrix is similar to exactly one matrix in rational canonical form. So we can restrict our attention to matrices in rational canonical form. Every such matrix is comprised of companion matrices along the diagonal whose associated polynomials are invariant factors and satisfy the familiar divisibility condition. The dimensions of the companion matrices are the same as the degrees of the associated polynomials:

\[ f_n(x) | \cdots | f_1(x) | f_0(x). \]

Now it is easy to see that the graph of any polynomial in $\mathbb{R}[x]$ of odd degree must cross the $X$-axis. This means that any polynomial of odd degree must have a (real) root. Constraint (c) tells us that none of the companion matrices involved here can have odd size.

Now the minimal polynomial is $f_0(x)$ and the characteristic polynomial is $f_{n-1}(x) \ldots f_1(x)f_0(x)$. Since we are looking for two dissimilar matrices, we must have a second sequence of polynomials $g_{m-1}(x) | \cdots | g_1(x) | g_0(x)$ as well.

The constraint (a) tells us that $f_0(x) = g_0(x)$. The constraint (b) tells us that $f_{n-1}(x) \ldots f_1(x)f_0(x) = g_{m-1}(x) \ldots g_1(x)g_0(x)$. Recall that constraint (c) entails that all these polynomials have even degree. We also know that they are all monic.

Now we have a trouble. What is the dimension of our matrices, i.e. what is the degree of the characteristic polynomial? The degrees of the minimal polynomial and of the characteristic polynomial must be even, in view of constraint (c). It is pretty clear that the dimension of our matrices cannot be 2. Can it be 4? In that case, the minimal polynomial must have either degree 4 and degree 2. It cannot be 4 since then it is also the characteristic polynomial and we see the $m = n = 0$. In other words, those divisibility chains only have one polynomial each. So there is only one rational canonical matrix rather than the two we need. On the other hand, if the degree is 2, then we see that $f_1(x)$ and $g_1(x)$ must also be of degree 2. This time the chains have just two polynomials apiece. Since we know $f_0(x) = g_0(x)$ and $f_1(x)f_0(x) = g_1(x)g_0(x)$, we also get $f_1(x) = g_1(x)$. So again there is only one rational canonical matrix.

How about $6 \times 6$? Just considering the sizes of the companion matrices, we see three schemes: the first giving one single $6 \times 6$ companion matrix, the second giving one of size $2 \times 2$ and a second of size $4 \times 4$, and the third scheme giving three companion matrices each of dimension $2 \times 2$. Under the first scheme the degree of the minimal polynomial will be 6, under the second it will be 4, and under the third it will be 2. So our counterexamples, having the same minimal polynomial, must both come from the same scheme. So we reject the first scheme outright. In the third scheme, since all the associated polynomials are monic, of the same degree, and satisfy the divisibility conditions, we see that they are all the same as the minimal polynomial. For this reason we reject the third scheme. Unfortunately, we have to reject the remaining possibility has well, since we know $f_0(x) = g_0(x)$ and $f_1(x)f_0(x) = g_1(x)g_0(x)$, we also get $f_1(x) = g_1(x)$. So again there is only one rational canonical matrix.

How about $8 \times 8$? Here we can succeed! Look at

\[ x^2 + 1 | x^2 + 1 | (x^2 + 1)^2 \quad \text{and} \quad (x^2 + 1)^2 | (x^2 + 1)^2. \]

Here the minimal polynomial is

\[ x^4 + 2x^2 + 1 = (x^2 + 1)^2 \]
and the characteristic polynomial is
\[ x^8 + 4x^6 + 6x^4 + 4x^2 + 1 = (x^2 + 1)^4. \]
The two dissimilar $8 \times 8$ matrices are displayed below.

\[
\begin{pmatrix}
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\quad \begin{pmatrix}
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\]

---

**Solutions to Algebra Homework, Edition 13**

27 January 2011

**Problem 42.**
Derive a list of equations that follow from the equations axiomatizing the theory of groups. This is rather open ended, but see if you can get a handful of useful looking equations.

**Solution**
I will list here without proof the equations that the class deduced from the group axioms, along with some others. Some of these were given inductive extensions.

\[
(xy)^{-1} = y^{-1}x^{-1} \\
(x^{-1})^{-1} = x \\
(x^n)^{-1} = (x^{-1})^n \\
x^{n}x^{m} = x^{n+m} \\
(xy^{-1})(xz^{-1}) = x(yz)x^{-1} \\
(xy^{-1})^{-1} = xy^{-1}x^{-1} \\
(xy^{-1})^n = xy^n x^{-1} \\
1^{-1} = 1 \\
(x^n)^m = x^{nm} \\
(xy)y^{-1} = x \\
(xy^{-1})y = x \\
x(x^{-1}y) = y \\
x^{-1}(xy) = y
\]
In the above list, \( n \) and \( m \) can be made to range over integers. Perhaps the best way to do this is to give some recursive definitions:

\[
\begin{align*}
x^0 &= 1 \\
x^{n+1} &= x^n x \text{ for every natural number } n \\
x^{-n} &= (x^{-1})^n \text{ for every natural number } n
\end{align*}
\]

Then the proofs should be accomplished by induction.

A number of people also included some interesting implications between equations.

**Problem 43.**
The five equations used to axiomatize groups are not all needed. Find a simpler set of equations that will serve.

**Solution**
Let’s show that the following three equations axiomatize the class of all groups.

\[
\begin{align*}
x(yz) &= (xy)z \\
x x^{-1} &= 1 \\
x1 &= x
\end{align*}
\]

What we need to do is derive the remaining two equations from these three. Here is a derivation of \( x^{-1}x = 1 \):

\[
x^{-1}x = x^{-1}(x1) = x^{-1}(x(x^{-1}(x^{-1})^{-1})) = x^{-1}((xx^{-1})(x^{-1})^{-1}) = x^{-1}(1(x^{-1})^{-1}) = (x^{-1})(x^{-1})^{-1} = x^{-1}(x^{-1})^{-1} = 1
\]

and here is the derivation of \( 1x = x \):

\[
1x = (xx^{-1})x = x(x^{-1}x) = x1 = x.
\]

**Problem 44.**
Prove that the additive group of all polynomials in \( x \) with integer coefficients is isomorphic to the multiplicative group of all positive rational numbers.

**Solution**
A polynomial with integer coefficients has the form

\[
a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n
\]

where \( a_0, a_1, \ldots, a_n \) are integers.

Let \( p_0, p_1, p_2, \ldots \) be the strictly ascending list of prime numbers. This list begins \( 2, 3, 5, 7, \ldots \). The isomorphism I have in mind sends the polynomial \( a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n \) to the positive rational \( p_0^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n} \). A delightful, routine effort by hard working graduate students will show that this map works.

**Problem 45.**
Let \( A \) and \( B \) be groups and let \( f : A \to B \). Prove that \( f \) is a homomorphism if and only if \( f(aa') = f(a)f(a') \) for all \( a, a' \in A \).
Solution
To verify that $f$ is a homomorphism it remains to show that $f(1) = 1$ and the $f(a^{-1}) = (f(a))^{-1}$. For the first observe that $1 \cdot f(1) = f(1) = f(1 \cdot 1) = f(1)$. Here we have used the assumption that $B$ is a group to say $1 \cdot f(1) = f(1)$ and the assumption that $A$ is a group to say $1 = 1 \cdot 1$. So we get $1 \cdot f(1) = f(1)$. Now use that $B$ is a group to cancel an $f(1)$ from both sides to get $1 = f(1)$.

Here is how to get the second conclusion.

$f(a) \cdot (f(a))^{-1} = 1 = f(1) = f(a \cdot a^{-1}) = f(a)f(a^{-1})$.

So we have $f(a) \cdot (f(a))^{-1} = f(a)f(a^{-1})$. Now cancel an $f(a)$ from both sides to get $(f(a))^{-1} = f(a^{-1})$, as desired. Observe that this line of reasoning relied as well on the fact the $A$ and $B$ we both groups.

Problem 46.
Let $A$, $B$, and $C$ be groups. Let $h$ be a homomorphism from $A$ onto $B$ and let $g$ be a homomorphism from $A$ onto $C$ such the $\ker h = \ker g$.

Prove that there is an isomorphism $f$ from $B$ onto $C$.

Solution
We know from the Homomorphism Theorem that $B \cong A/\ker h$ and that $C \cong A/\ker g$. Because $\ker h = \ker g$ we see

$$B \cong A/\ker h = A/\ker g \cong C.$$ 

So $B$ and $C$ must be isomorphic.

-----

Solutions to Algebra Homework, Edition 14
3 February 2011

Problem 47.
Prove that every group that has a proper subgroup of finite index must have a proper normal subgroup of finite index.

Solution
Let $G$ be a group and let $H$ be a proper subgroup of $G$ of finite index. Let $\mathcal{X}$ be the collection of left cosets of $H$. So $\mathcal{X}$ is finite. Therefore $\text{SYM}\mathcal{X}$ is also finite. Let $G$ act on $\mathcal{X}$ by left translation. Let $N$ be the kernel of this action. Then $N$ is a normal subgroup of $G$ and since $G/N$ is isomorphic to a subgroup of the finite group $\text{SYM}\mathcal{X}$, we see that the index of $N$ in $G$ is finite. It remains to show that $N$ is a proper subgroup of $G$. Since $H$ is a proper subgroup of $G$ pick $a \in G$ with $a \notin H$. So left translation by $a$ sends $H$ to $aH$. This means that left translation by $a$ is not the identity map. Thus $a \notin N$ and $N$ is a proper subgroup of $G$.

Problem 48.
Let $G$ be a group. Prove that $G$ cannot have four distinct proper normal subgroups $N_0, N_1, N_2,$ and $N_3$ so that $N_0 \leq N_1 \leq N_2 \leq G$ and so that $N_1 N_3 = G$ and $N_2 \cap N_3 = N_0$. 

Solution
For the sake of contradiction, suppose that there are such subgroups. We contend that \( N_2 \subseteq N_1 \), which is a contradiction. To see this, let \( a \in N_2 \). Since \( N_2 \subseteq N_1 N_3 \), pick \( b \in N_1 \) and \( c \in N_3 \) so that \( a = bc \). Consequently \( b^{-1}a = c \). Since \( N_1 \subseteq N_2 \) and since \( N_1 \) and \( N_2 \) are subgroups we have that \( b^{-1}a \in N_2 \). Therefore, \( b^{-1}a = c \in N_2 \cap N_3 \). But \( N_2 \cap N_3 \subseteq N_1 \). So \( b^{-1}a = c \in N_1 \). Now recall that \( b \in N_1 \) as well. So \( a = bc \in N_1 \) and this means \( N_2 \subseteq N_1 \) just as we contended.

Problem 49.
Let \( H \) and \( K \) be subgroups of the group \( G \) each of finite index in \( G \). Prove that \( H \cap K \) is also a subgroup of finite index in \( G \).

Solution
It helps to know the following fact:

If \( G \) is a group and \( M \leq L \leq G \), then \( [G : M] = [G : L][L : M] \).

I sketch a proof of this at the end of this solution.

According the the fact displayed above \( [G : H \cap K] = [G : H][H : H \cap K] \). We know that \( [G : H] \) is finite, it is enough to show that \( [H : H \cap K] \) is finite. Now we also know that \( [G : K] \) is finite. It follows that \( \{aK \mid a \in H \} \) is also finite. This entails that \( \{aK \cap H \mid a \in H \} \) is finite as well. But observe that for \( a \in H \) we have

\[
b \in aK \cap H \iff b \in H \text{ and } b = ak \text{ for some } k \in K
\]

\[
\iff b \in H \text{ and } a^{-1}b \in K \iff a^{-1}b \in H \cap K \iff b \in a(H \cap K)
\]

So for \( a \in H \) we have that \( aK \cap H = a(H \cap K) \). This means that \( \{a(H \cap K) \mid a \in H \} \) is finite. This is just another way to say that \( [H : H \cap K] \) is finite.

Now let’s sketch out why \( [G : M] = [G : L][L : M] \) as stated above. We start by selecting a representative element from each left coset of \( L \). Now define the map \( \Phi \) as follows

\[
\Phi(aM) = (aL, r^{-1}aM) \text{ where } r \text{ is the representative of } aL.
\]

We intend for \( \Phi \) to be a one-to-one map from the collection of left cosets of \( M \) onto the set of ordered pairs of left cosets of \( L \) with left cosets of \( M \) in \( L \). Thus we must show that the definition of \( \Phi \) is sound, that \( \Phi \) is one-to-one, and that \( \Phi \) is onto. To see that the definition is sound, suppose \( aM = a'M \). Evidently, \( r^{-1}aM = r^{-1}a'M \). Also, since \( M \subseteq L \) we see that \( aM \subseteq aL \) and \( a'M \subseteq a'L \). Since the left cosets of \( L \) constitute a partition, we conclude that \( aL = a'L \). This means \( (aL, r^{-1}aM) = (a'L, r^{-1}a'M) \) and our definition is sound. To secure the one-to-oneness, suppose \( \Phi(aM) = \Phi(a'M) \).

So \( aL = a'L \) (which means we are using the same \( r \)) and \( r^{-1}aM = r^{-1}a'M \). But just multiply this last equation by \( r \) of the left to obtain \( aM = a'M \). So \( \Phi \) is one-to-one. Finally, to establish the ontoness, let \( aL \) be a left coset of \( L \) and \( bM \) be a left coset of \( M \) where \( b \in L \). Let \( r \) be the representative of \( aL \). So \( aL = rL = rbL \), since \( b \in L \). Now observe

\[
\Phi(rbM) = (rbL, r^{-1}rbM) = (aL, bM).
\]

Therefore \( \Phi \) has all the desired properties and \( [G : M] = [G : L][L : M] \) as desired.

Problem 50.
Prove that there is no group \( G \) such that \( G/Z(G) \cong \mathbb{Z} \), where \( \mathbb{Z} \) denotes the group of integers under addition.
Solution

Something stronger is true: if $G/Z(G)$ is a cyclic group, then it is trivial and $G$ must be Abelian.

Since $G/Z(G)$ is cyclic we can pick $b \in G$ so that $\{a^nZ(G) \mid n \in \mathbb{Z}\}$ is the whole quotient group. In this way $aZ(G)$ is a generator of this cyclic group. To see that $G$ is Abelian, let $b, c \in G$. So these elements belong to cosets of the center, and so it is possible to pick integers $n$ and $m$ and also $z_0, z_1 \in Z(G)$ so that $b = a^n z_0$ and $c = a^m z_1$. Now just compute

$$bc = a^n z_0 a^m z_1 = a^n a^m z_1 z_0 = a^{n+m} z_1 z_0 = a^m z_1 a^n z_0 = cb.$$ 

So $G$ is Abelian, $G = Z(G)$ and $G/Z(G)$ is trivial.

Solutions to Algebra Homework, Edition 15
10 February 2011

Problem 51.
Let $p$ be the smallest prime that divides the cardinality of the finite group $G$. Prove that any subgroup of $G$ of index $p$ must be normal.

Solution

Let $H$ be a subgroup of $G$ of index $p$. Let $\mathcal{X} = \{aH \mid a \in G\}$. Then $|\mathcal{X}| = p$ and $|\text{SYM}\mathcal{X}| = p!$. Let $G$ act on $\mathcal{X}$ by left translation and let $N$ be the kernel of this action. Then $[G : N] \mid p!$. Since $p$ is the least prime dividing $|G|$ we see that the only possibilities for $[G : N]$ are 1 and $p$. But observe

$$b \in N \iff baH = aH \text{ for all } a \in G$$

$$\iff a^{-1}ba \in H \text{ for all } a \in G$$

$$\Rightarrow b \in H \text{ (take } a = 1)$$

So $N \leq H$. Since $[G : N] = [G : H][H : N] = p'[H : N]$. Thus $[G : N]$ cannot be 1 and therefore must be $p$. But now we have $N \leq H \leq G$ where $G$ is finite and $H$ and $N$ are both of index $p$. It follows that $|N| = |H|$. Since everything is finite we conclude that $N = H$ and so $H$ is a normal subgroup of $G$.

Problem 52.
How many elements of order 7 are there in a simple group of order 168?

Solution

Observe that $168 = 2^3 \cdot 3 \cdot 7$. Now any element of order 7 must belong to a subgroup of order 7. Let $n$ be the number of 7-Sylow subgroups of our simple group. Then $n \equiv 1 \mod 7$ and $n \mid 28$. These two constraints tell us that $n = 1$ or $n = 8$. But $n = 1$ is impossible since the group is simple (and so cannot have a proper nontrivial normal subgroup). So our group has 8 subgroups of order 7. Since 7 is prime, each of these groups is generated by any of its elements except for the identity element 1. This means that the intersection of any two distinct 7-subgroups must be trivial. Now each of the eight 7-subgroups has six elements of order 7. So our simple group has $8 \cdot 6 = 48$ elements of order 7.
Problem 53.
Let $N$ be a normal subgroup of the finite group $G$ and let $K$ be a $p$-Sylow subgroup of $N$ for some prime $p$. Prove that $G = N_G(K)N$.

Solution
Let $a \in G$. Because $N$ is a normal subgroup of $G$ we have $a^{-1}Ka \subseteq a^{-1}Na = N$. So $a^{-1}Ka$ is a $p$-Sylow subgroup of $N$. But according to the Sylow Theorem, any two $p$-Sylow subgroup of $N$ are conjugate (with respect to $N$). So pick $b \in N$ so that $a^{-1}Ka = bKb^{-1}$. But this means $ab^{-1}K(ab^{-1})^{-1} = K$. Therefore $ab^{-1} \in N_G(K)$. Since $a = ab^{-1}b$ we have that $a \in N_G(K)N$. Thus $G$ is a subgroup of $N_G(K)N$. Since the reverse inclusion is obvious, we have $G = N_G(K)N$ as desired.

Problem 54.
Prove that there is no simple group of order 56.

Solution
Observe that $56 = 2^3 \cdot 7$. Suppose, for the sake of contradiction, that $G$ is a simple group of order 56. Let $n_2$ be the number of 2-Sylow subgroups and $n_7$ be the number of 7-Sylow subgroups. Since $G$ is simple, neither $n_2$ nor $n_7$ can be 1. Now according to Sylow, $n_2$ is odd and divides 7. So $n_2 = 7$. Also according to Sylow, $n_7 \equiv 1 \mod 7$ and $n_7 | 8$. Hence $n_7 = 8$. Now the 7-Sylow subgroups, being cyclic of prime order must have pairwise trivial intersections. This means that the number of elements of order 7 in $G$ is $8 \cdot 6 = 48$. Now each of the 2-Sylow subgroups is of order 8. Let $H$ and $K$ be distinct 2-Sylow subgroups. Let $a \in K$ with $a \notin H$. Now let us count elements. There is 1 element of order 1, namely the identity element. There are 48 elements of order seven. $H$ has 7 elements different from the identity element and which have orders dividing 8 (so they have not been counted before). Finally there is at least one more element, namely $a$. Altogether this gives $1 + 48 + 7 + 1 = 57$. But $G$ has only 56 elements and we have reached a contradiction.

Problem 55.
Prove that if $G$, $H$, and $K$ are finite Abelian groups and $G \times H \cong G \times K$, then $H \cong K$.

Solution
For any finite Abelian group $L$, let $n_L(q)$ be the number of directly indecomposable factors of order $q$ in any direct decomposition of $L$ into directly indecomposable groups. According to the Fundamental Theorem for Finite Abelian Groups, $n_L$ is well-defined and provides a complete system of invariants for $L$. To see that $H \cong K$ it suffices to show that $n_H(q) = n_K(q)$ for ever prime power $q$. However, since $G \times H \cong G \times K$ we know that

$$n_G(q) + n_H(q) = n_{G \times H}(q)$$
$$= n_{G \times K}(q)$$
$$= n_G(q) + n_K(q)$$
But this means \( n_G(q) + n_H(q) = n_G(q) + n_K(q) \). This entails \( n_H(q) = n_K(q) \) as desired.

**Problem 56.**
Prove that every group of order 35 is cyclic.

**Solution**
Observe that 35 = 5 \cdot 7. Let \( G \) be a group of order 35. Let \( n_5 \) be the number of 5-Sylow subgroups of \( G \) and let \( n_7 \) be the number of 7-Sylow subgroups of \( G \). We know that \( n_5 \equiv 1 \mod 5 \) and that \( n_5 | 7 \). Consequently, \( n_5 = 1 \). Let \( H \) be the unique 5-Sylow subgroup of \( G \). We know that \( H \) is a normal subgroup of \( G \) and that \( H \) is just the cyclic group of order 5. Likewise, we know that \( n_7 \equiv 1 \mod 7 \) and that \( n_7 | 5 \). Hence, \( n_7 = 1 \) as well. Let \( K \) be the unique 7-Sylow subgroup of \( G \). Then \( K \) is a normal subgroup of \( G \) and it is just the cyclic group of order 7. According to Lagrange the intersection of these two normal subgroups must be trivial, since any shared elements must have an order that divides both 5 and 7. It now follows from our Isomorphism Theorems that \( |HK| = 5 \cdot 7 = 35 \). Since \( G \) is finite, this forces \( G = HK \). Therefore \( G \cong H \times K \). This means that \( G \) is a finite Abelian group. It admits only one direct factorization into directly indecomposable groups—the one just given. This means that up to isomorphism, there is only one Abelian group of order 35. Since the cyclic group of order 35 is Abelian, we find that \( G \) is cyclic. Another way to see that \( G \) is cyclic is to let \( a \) generate \( H \) and \( b \) generate \( K \). Then \( a \) has order 5 and \( b \) has order 7. One can then prove that the order of \( ab \) is the least common multiple of 5 and 7. This least common multiple of course 35 so \( ab \) generated \( G \).

**Problem 57.**
Describe, up to isomorphism, all groups of order 1225.

**Solution**
Observe 1225 = 5^2 \cdot 7^2. Let \( G \) be a group of order 1225. Let \( n_5 \) and \( n_7 \) be the number of 5-Sylow and the number of 7-Sylow subgroups of \( G \), respectively. By Sylow we know that \( n_5 \equiv 1 \mod 5 \) and \( n_5 | 49 \). Likewise \( n_7 \equiv 1 \mod 7 \) and \( n_7 | 25 \). Thus, \( n_5 = 1 = n_7 \). So let \( H \) be the unique 5-Sylow subgroup. It is a normal subgroup of order 25. Likewise, let \( K \) be the unique 7-Sylow subgroup. It is a normal subgroup of order 49. Since 25 and 49 are relatively prime, Lagrange assures us that \( H \) and \( K \) have a trivial intersection. By our isomorphism theorems, \(|HK| = |H||K|\) and since \(|G| = 25 \cdot 49 = |H||K| = |HK|\) we see that \( G = HK \). This means that \( G = H \otimes K \). Now both \( H \) and \( K \) must be Abelian, since their order are \( p^2 \) for certain primes \( p \). This means that \( G \) must be an Abelian group of order 1225. According to the Fundamental Theorem of Finite Abelian Groups such a group must be isomorphic to one the four listed below, and no two of those listed are isomorphic to each other. This list amounts to a description, up to isomorphism of all the groups of order 1225.

\[
\begin{align*}
C_{25} \times C_{49} & \quad C_5 \times C_5 \times C_{49} \\
C_{25} \times C_7 \times C_7 & \quad C_5 \times C_5 \times C_7 \times C_7
\end{align*}
\]

In this list \( C_n \) denotes the cyclic group of order \( n \).

**Problem 58.**
Let \( G \) be a finite Abelian group. Prove that if \(|G|\) is not divisible by \( k^2 \) for any \( k > 1 \), then \( G \) is cyclic.
Solution

The divisibility condition means that \(|G| = p_0 p_1 \cdots p_{n-1}\) where \(p_0, p_1, \ldots, p_{n-1}\) are distinct primes. For each \(i < n\) let \(N_i\) be the \(p_i\)-Sylow subgroup of \(G\) (which we know from Sylow is unique since it is normal). We proved in class that every finite Abelian group is the internal direct product of its Sylow subgroups, so \(G = N_0 \otimes N_1 \otimes \cdots \otimes N_{n-1}\). Now each of these Sylow subgroups, being of prime order, is cyclic. For each \(i < n\) let \(a_i\) generate \(N_i\). We contend that \(a_0 a_1 \cdots a_{n-1}\) generates \(G\). Suppose \((a_0 a_1 \cdots a_{n-1})^m = 1\). This entails that \(a_0^m a_1^m \cdots a_{n-1}^m = 1\) and so also \(a_0^m = a_1^{-m} a_2^{-m} \cdots a_{n-1}^{-m}\). Because \(N_0\) and \(N_1 N_2 \cdots N_{n-1}\) have a trivial intersection this means that \(a_0^m = 1\). Similar arguments show that \(a_i^m = 1\) for all \(i < n\). This means that \(p_i \mid m\) for all \(i < n\). By relative primeness this means that \(|G| = p_0 p_1 \cdots p_{n-1} \mid m\). So we see that \(|G|\) divides the order of \(a_0 a_1 \cdots a_{n-1}\). But by Lagrange, the order of \(a_0 a_1 \cdots a_{n-1}\) also divides \(|G|\). So the element \(a_0 a_1 \cdots a_{n-1}\) has order \(|G|\) and so generates the whole group \(G\). So \(G\) is cyclic.

Solutions to Algebra Homework, Edition 17
24 February 2011

Problem 59.

Prove that \(\text{Aut}(S_n) \cong S_n\), for ever natural number \(n\), except when \(n = 2\) or \(n = 6\). You can use, without proof, that if \(n \neq 6\) then, in \(S_n\), the image, under any automorphism, of any transposition is again a transposition.

Solution

Let \(S_n\) act on \(S_n\) by conjugation and let \(F\) be the underlying homomorphism. So \(F\) maps \(S_n\) into \(\text{Aut}(S_n)\). It remains to show that \(F\) is one-to-one and onto.

Here is why it is one-to-one:

\[
F_\sigma = \text{Id}_{\text{Aut}(S_n)} \iff \sigma \circ \tau \circ \sigma^{-1} = \tau \text{ for all } \tau \in S_n \\
\iff \sigma = \text{Id}_{S_n}
\]

The last equivalence may need some justification. Suppose that \(\sigma \neq \text{Id}_{S_n}\) and pick \(a, b\) so that \(\sigma(a) = b\) where \(a \neq b\). Pick \(c \notin \{a, b\}\). Let \(\tau = (b, c)\). Then \(\sigma(\tau(\sigma^{-1}(b))) = \sigma(\tau(a)) = \sigma(a) = b \neq c = \tau(b)\). So \(\sigma \circ \tau \circ \sigma^{-1} \neq \tau\). In this way we see that \(\ker F\) is trivial, so \(F\) is one-to-one. In fact, what we argued here is the center \(Z(S_n)\) is trivial. Of course, we used in this argument that \(n \geq 3\) (to pick that third element \(c\)). So what about \(n = 0, 1\) and \(2\)? Well, \(S_n\) in the first two of these cases is the trivial group (which is evidently isomorphic to its group of automorphisms). What happens if \(n = 2\)? Observe that \(S_2\) is the group with two elements. Now any automorphism must take the identity element to itself. Since there is only one other element and automorphisms have to be one-to-one, that element must map to itself has well: the only automorphism is the identity map. This means that \(\text{Aut}(S_2)\) has only one element, while \(S_2\) has two elements. They cannot be isomorphic.

Recall that

\[
G/\mathbb{Z}(G) \cong \text{Inn}(G).
\]

For \(G = S_n\) with \(n \neq 2\), we argued that the center is trivial. So

\[
S_n \cong \text{Inn} S_n.
\]

We would like to prove that \(F\) is onto or, what is the same, that every automorphism of \(S_n\) is an inner automorphism.
Consider for the moment that \( \sigma \in S_n \) and that \( a, b \in \{0, \ldots, n-1\} \) with \( a \neq b \). An easy direct calculation shows
\[
\sigma \circ (a, b) \circ \sigma^{-1} = (\sigma(a), \sigma(b)).
\]
So we see that conjugating a transposition always results in a transposition. Our unproven assumption in the problem is that this applies not only to the inner automorphisms, but to all automorphisms.

Let \( \varphi \) be an automorphism of \( S_n \).

Consider the transpositions \((0,1), (1,2), \ldots, (n-2,n-1), (n-1,0)\). It turns out that these transpositions generate the whole group \( S_n \). This means that \( \varphi \) is entirely determined by what it does to the transpositions listed. Now \((0,1)(1,2) = (0,1,2)\) which is an element of order 3. Using our assumption, let \( \varphi(0,1) = (a, b) \) and \( \varphi(1,2) = (c, d) \). It follows that \((a, b)(c, d)\) must be an element of order 3. Hence, \((a, b)\) and \((c, d)\) must be distinct transpositions which are not disjoint. Let us suppose that \( b = c \) while \( a \neq d \). Then we can enumerate these three elements as \( a_0 = a, a_1 = b, \) and \( a_2 = d \).

Now consider \((1,2)(2,3)\). By our assumption, let \( \varphi(2,3) = (u,v) \). Again \((a_1, a_2)\) and \((u,v)\) must be distinct transpositions which are not disjoint. On the other hand, \((a_0, a_1)(u,v)\) must have order 2 since \((0,1)(2,3)\) has order 2. This forces \( a_2 \in \{u,v\} \). Say \( u = a_2 \) and rename \( v \) as \( a_3 \). We continue in this way. More precisely, at stage \( k \) we have at hand \( a_0, a_1, \ldots, a_k \) so that

- \( \varphi(i, i+1) = (a_i, a_{i+1}) \) for each \( i < k \) and
- \( a_0, \ldots, a_k \) are pairwise distinct.

If \( k = n-1 \), we are at the end of our construction. If \( k < n-1 \) we can continue as follows. Let \( \varphi(k, k+1) = (u,v) \). Now \((k-1, k)(k, k+1) = (k-1, k, k+1)\) which has order 3 and, on the other hand, \((j, j+1)(k, k+1)\) has order 2 when \( j + 1 < k \). This means \((a_{k-1}, a_k)(u,v)\) must have order 3 and, on the other hand, \((a_j, a_{j+1})(u,v)\) has order 2 when \( j + 1 < k \). Consequently, \( u \) and \( v \) cannot occur among \( a_0, \ldots, a_{k-1} \) but one of \( u \) or \( v \) must be \( a_k \). Let \( a_{k+1} \) be the other of \( u \) and \( v \).

Now let \( \sigma \) be the permutation of \( \{0, \ldots, n-1\} \) such that \( \sigma(i) = a_i \) for all \( i < n \). Just observe
\[
\varphi(i, i+1) = (a_i, a_{i+1}) = (\sigma(i), \sigma(i+1)) = \sigma \circ (i, i+1) \circ \sigma^{-1}.
\]
This means that \( \varphi \) is indeed an inner automorphism.

Here is the missing piece I didn’t ask you to prove.

**Lemma about transpositions.** Let \( n \) be a natural number with \( n \neq 6 \) and let \( \varphi \in \text{Aut} S_n \). The image, with respect to \( \varphi \), of any transposition must be a transposition.

Here we take \( n \neq 6 \) and let \( \varphi \) be any automorphism of \( S_n \). Now any transposition has order 2 and so its image under \( \varphi \) must also have order 2. It is too bad that being of order 2 does not characterize the transpositions. We need some additional property.

Suppose \( \tau \in S_n \) is an permutation of order 2. By considering the decomposition of \( \tau \) into disjoint cycles, we see that \( \tau \) must be a product of disjoint transpositions. Let \( k \) be the number of these transpositions. Now, since the conjugate of a transposition is again a transposition, any conjugate of \( \tau \) must also be a product of \( k \) disjoint transpositions. It is not too hard to see that the converse of this statement is also true: if \( \rho \) is the product of \( k \) disjoint transpositions then \( \rho \) is a conjugate of \( \tau \).

[Just line up the factorizations, one above the other, to see the permutation \( \sigma \) to use in forming the conjugate.]

So how big is the conjugacy class of \( \tau \)? One thing we know: \( 2k \leq n \). Let us count the number of ways to choose \( k \) disjoint subsets of \( \{0, \ldots, n-1\} \) each with 2 elements. There are
\[
\binom{n}{2} = \frac{n(n-1)}{2}
\]
ways to choose the first 2-element subset. Next, there are
\[
\binom{n-2}{2} = \frac{(n-2)(n-3)}{2}
\]
ways to choose the next one. Continuing in this ways to choose \( k \) of them we arrive at

\[
\frac{n!}{2^k(n-2k)!k!}
\]

But the order in which we made our choices has no effect on the resulting selection. Taking this into account, we see that the conjugacy class of \( \tau \) has

\[
\frac{n!}{2^k(n-2k)!k!}
\]

members.

Now if \( \tau \) is a transposition, then \( k = 1 \) and this number becomes

\[
\frac{n!}{2(n-2)!}.
\]

The automorphism \( \varphi \) must induce a one-to-one correspondence between the conjugacy class of \( \tau \) and the conjugacy class of \( \varphi(\tau) \). Suppose \( \varphi(\tau) \) is the product of \( k \) disjoint transpositions. This gives us the following equivalent equations:

\[
\frac{n!}{2(n-2)!} = \frac{n!}{2^k(n-2k)!k!}
\]

\[
2^k(n-2k)!k! = 2(n-2)!
\]

Observe that this last equality holds when \( n = 6 \) and \( k = 3 \). This case is rejected, since \( n \neq 6 \) This is the only place we use this stipulation. We must reject all the \( k \)'s so that \( 1 < k \) and \( 2k \leq n \).

Consider first the case when \( k = 2 \). Our equations becomes \( 4(n-4)! = (n-2)! \), which yields \( 4 = (n-2)(n-3) \). This is certainly false.

So suppose \( 3 \leq k \). Then \( 6 < n \).

It helps to observe

\[
1 \leq \binom{n-k}{k} = \frac{(n-k)!}{k!(n-2k)!}
\]

\[
2^{k-1}(n-2k)!k! \leq 2^{k-1}(n-k)!
\]

So our purposes will be served if we can show

\[
2^{k-1} < \frac{(n-2)!}{(n-k)!}
\]

Or what is the same

\[
2^{k-1} < (n-2)(n-3)\ldots(n-k+1).
\]

On the right there are \( k-2 \) factors. The smallest one is \( n-k+1 \geq 2k-k+1 = k+1 \geq 4 \). This means the left side is at greater than \( 4^{k-2} = 2^{2k-4} \). But \( 2k-4 \geq k-1 \). So the desired inequality holds.

All this means that \( k = 1 \) and \( \varphi(\tau) \) is a transposition, as desired.

So now we know that every automorphism of \( S_n \) is an inner automorphism, at least when \( n \neq 6 \). Our proof breaks down when \( n = 6 \) and we are left in ignorance. To cure this ignorance we will show that \( S_6 \) has an automorphism which is not an inner automorphism. The was first established in 1895 by Otto Hölder.

First consider \( S_5 \). This group contains exactly \( 24 = 4! \) elements of order 5. They are just the 5-cycles. Let \( n_5 \) be the number of Sylow 5-subgroups of \( S_5 \). We know that each is of order 5 and that \( n_5 \equiv 1 \mod 5 \) and that \( n_5 \) divides 24. Thus \( n_5 = 1 \) or \( n_5 = 6 \). The first alternative cannot account for all those elements of order 5. So it must be that \( n_5 = 6 \). If we let \( S_5 \) act on its Sylow 5-subgroups by conjugation we see, by Sylow’s Theorems, that there is just one orbit \( O \). Let \( \Phi \) be the action of \( S_5 \) on
Let us say that \( O \) by conjugation. Actually, Sylow’s Second Theorem tells us that every member of \( O \) can be mapped to any other element of \( O \) by conjugation, so the image of \( S_5 \) under \( \Phi \), which is a subgroup of \( \text{Sym} O \), has at least 6 elements. Now the kernel \( \Phi \) is a normal subgroup of \( S_5 \) so it must either be trivial or \( S_5 \) itself or \( A_5 \), this being the complete list of normal subgroups of \( S_5 \). By Lagrange, this entails that the kernel is trivial. But this means that \( \Phi \) embeds \( S_5 \) into \( \text{Sym} O \). Moreover, Sylow tells us that the image of \( S_5 \) in \( \text{Sym} O \) is transitive in the sense that given \( P, P' \in O \), there is \( \sigma \) in the image of \( S_5 \) that sends \( P \) to \( P' \).

Recalling that \( |O| = 6 \), we conclude that \( S_6 \) has a subgroup \( H \) that is transitive and isomorphic to \( S_5 \). In particular, \( |H| = 5! = 120 \) and \( |S_6 : H| = 6 \).

Now let \( U \) be the collection of conjugates of \( H \) by members of \( S_6 \). Let \( \Psi \) be the action of \( S_6 \) by conjugation on \( U \). The Key Fact about orbits tells us

\[
|U| = [S_6 : N(H)]
\]

where \( N(H) \) is the normalizer of \( H \) in \( S_6 \). So we see

\[
6 = [S_6 : H] = [S_6 : N(H)][N(H) : H] = |U||N(H) : H|.
\]

Now a bit of fiddling, done by eager graduate students, shows that \( \ker \Psi \subseteq N(H) \). Of course, \( \ker \Psi \) is also a normal subgroup of \( S_6 \), giving us three cases:

**Case:** \( \ker \Psi = S_6 \)

In this case, we would have \( N(H) = S_6 \), but then \( H \) would be a normal subgroup of \( S_6 \). This is impossible, since \( S_6 \) has precisely 3 normal subgroups: the trivial subgroup, \( A_6 \) and \( S_6 \) itself. \( H \) is not on this list—it is the wrong size. So this case is rejected.

**Case:** \( \ker \Psi = A_6 \)

Since \( A_6 \) has index 2 in \( S_6 \), that can be no subgroups properly between \( A_6 \) and \( S_6 \). Since we saw above that \( N(H) \neq S_6 \), we are forced to conclude that \( A_6 = N(H) \). This would make \( H \triangleleft A_6 \), but \( A_6 \) is simple, having only itself and the trivial group as its normal subgroups. So we have to reject this case as well.

The only case remaining is that \( \ker \Psi \) is trivial. This case must hold true. So \( \Psi \) embeds \( S_6 \) into \( \text{Sym} U \). This means that \( |U| \) is at least 6. But we saw above that \( |U| \) is a factor of 6. So \( |U| = 6 \).

Considering that the sets involved are finite, we see that \( \Psi \) is an isomorphism from \( S_6 \) onto \( \text{Sym} U \). Further, we conclude that \( N(H) = H \).

Say \( U = \{H_0, \ldots, H_5\} \) where \( H = H_0 \) and the other \( H_i \)'s are the conjugates of \( H \). The map sending \( H_i \mapsto i \), induces an isomorphism from \( \text{Sym} U \) onto \( S_6 \). So the compositie map \( \Theta \circ \Psi \) is an automorphism of \( S_6 \). This is finally our candidate for an outer automorphism.

Let us suppose, to the contrary, that \( \Theta \circ \Psi \) is an inner automorphism, that it is conjugation by \( \alpha \) for some particular \( \alpha \in S_6 \). Now conjugation always takes a transposition to a transposition. So \( \Theta(\Psi((0,1))) \) must be a transposition. But is \( S_6 \) any transposition fixes 4 of the elements. Pulling this fact back through \( \Theta \) to \( \text{Sym} U \) we see that \( \Psi((0,1)) \) must fix four of the elements of \( U \). That is, for such an \( H_i \) we have \( (0,1)^{-1}H_i(0,1) = H_i \). Now pick \( \beta \in S_6 \) so that \( H_i = \beta^{-1}H_i\beta \). A finger twiddle gives \( \beta^{-1}(0,1)\beta \in N(H) \). But we saw above that \( N(H) = H \) and we know that any conjugate of a transposition is a transposition. This means that \( H \) contains a transposition.

So here is what we know about \( H \):

a) \( |H| = 120 \), so by Cauchy \( H \) has an element of order 5.

b) \( H \) contains a 5-cycle, these being the only elements of \( S_6 \) that have order 5.

c) \( H \) has a transposition.

d) \( H \) is transitive.

Let us say that \( (0,1,2,3,4) \in H \) and that \( (i,j) \in H \) with \( i \neq j \). Also, by transitivity, pick \( \gamma \in H \) so that \( \gamma(5) = i \). Then \( \gamma^{-1}(i,j)\gamma = (k,5) \) for some \( k \neq 5 \). By taking conjugates of \( (k,5) \) by appropriate powers of \( (0,1,2,3,4) \) we find inside \( H \) all the transpositions \( (0,5), (1,5), (2,5), (3,5), \) and \( (4,5) \). But
actually, if you look back at how we showed that every permutation could be written as a product of transpositions, you will see that this set of 5 transpositions actually generates $S_6$. Our conclusion? It is that $H = S_6$ and this is surely wrong. So we must reject the idea that $\Theta \circ \Psi$ is an inner automorphism.

---

**Problem 60.**
Let $p$ be a prime number. Prove that if $a$ and $b$ are elements of the symmetric group $S_p$, where $a$ has order $p$ and $b$ is a transposition, then $\{a, b\}$ generates $S_p$.

**Solution**
Recall that every member of $S_p$ can be written as a product of disjoint cycles and these commute with each other. Suppose $\tau$ is a permutation such that it decomposes into disjoint cycles all of length strictly less than $p$. Let $m$ be the product of the lengths of these cycles. Using the fact that disjoint cycles commute shows that the order of $\tau$ must divide $m$. But $p$ cannot divide $m$. So the order of $\tau$ cannot be $p$. This means that the only elements of $S_p$ which have order $p$ are the cycles of length $p$. So $a$ is a cycle of length $p$.

Now we also know that every permutation is a product of transpositions. So it is enough to show that every transposition is generated by $a$ and $b$. Without loss of generality we suppose that

$$a = (0, 1, 2, \ldots, p - 1) \quad b = (i, j) \text{ with } i < j < p$$

and that $(k, \ell)$ with $k < \ell < p$ is another transposition.

The first step is to prove (by induction on $r$) that $a^r b a^{-r} = (i + r, j + r)$ where the additions $i + r$ and $j + r$ work modulo $p$. As $r$ runs from $0$ to $p - 1$ notice that $i + r$ also takes on all the values from $0$ to $p - 1$ (although it starts at $i$). In this way we get all the transpositions of the form $(s, s + m)$ where $m = j - i$ and $s$ runs from $0$ to $p - 1$ and $s + m$ is taken modulo $p$. Now notice

$$(k + m, k + 2m)(k, k + m)(k + m, k + 2m) = (k, k + 2m)$$

$$(k + 2m, k + 3m)(k, k + 2m)(k + 2m, k + 3m) = (k, k + 3m)$$

$$\vdots$$

$$= (k, k + tm)$$

where $t$ is any positive integer but $k + tm$ is calculated modulo $p$. This means that all the transposition $(k, k + tm)$ have been generated from $a$ and $b$ where $t$ in any natural number. But now notice by Lagrange, $p$ is prime, that $m, 2m, 3m, \ldots, tm, \ldots$ must also run through all the values from $0$ to $p - 1$. Therefore the same applies to $k + tm$ as $t$ varies. So for the appropriate choice of $t$ we get $k + tm = \ell$. And we have generated $(k, \ell)$ as desired.

---

**Problem 61.**
Let $H \leq G$. Prove that $N_G(H)/C_G(H)$ is embeddable into $\text{Aut}(H)$.

**Solution**
Recall that $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ while $C_G(H) = \{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\}$. Now let $N_G(H)$ act on $H$ by conjugation and let $F$ be the underlying homomorphism. That if $F : N_G(H) \to \text{Aut}(H)$ where, for each $g \in N_G(H)$ and each $h \in H$ we have

$$F_g(h) = ghg^{-1}.$$ 

Notice that $F_g : H \to H$ since $g \in N_G(H)$. 

We can finish the problem using the Homomorphism Theorem by showing that \( \ker F = C_G(H) \). Here is the reasoning:

\[
g \in \ker F \iff F_g \text{ is the identity map on } H \\
\iff F_g(h) = h \text{ for all } h \in H \\
\iff ghg^{-1} = h \text{ for all } h \in H \\
\iff g \in C_G(H)
\]

From the Homomorphism Theorem we know that \( N_G(H)/C_G(H) \) is isomorphic to the image of \( N_G(H) \) with respect to \( F \). But this image is a subgroup of \( \text{Aut}(H) \). Thus \( N_G(H)/C_G(H) \) is isomorphic with a subgroup of \( \text{Aut}(H) \). That is, \( N_G(H)/C_G(H) \) is embeddable into \( \text{Aut}(H) \).

This problem gives you some idea of how an automorphism of \( H \) might arise that is not an inner automorphism of \( H \)—even those it is the restriction to \( H \) of an inner automorphism of the larger group \( G \).

**Problem 62.**

Let \( G \) be a group of order \( n \). Define \( \varphi : G \to G \) by \( \varphi(a) = a^{n^2+3n+1} \) for all \( a \in G \). Prove that \( \varphi \) is an automorphism of \( G \).

**Solution**

According to Lagrange, if \( G \) is a finite group with \( n \) elements, then the cardinality of any subgroup of \( G \) must divide \( n \). This includes all the subgroups generated by single elements. For any element \( a \in G \) the order of \( a \) is the size of the subgroup it generates. So the order of each element of \( G \) must divide \( n \). This means

\[
\varphi(a) = a^{n^2+3n+1} = (a^n)^n(a^3)^n = 1 \cdot 1 \cdot a = a.
\]

Thus, \( \varphi \) is just the identity map on \( G \). The identity map is always an automorphism.
In Problem 61 to Problem 66 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

\[ X \rightarrow = \{ b \mid x R b \text{ for all } x \in X \} \]
\[ Y \leftarrow = \{ a \mid a R y \text{ for all } y \in Y \} \]

**Problem 63.**
Prove that if $W \subseteq X \subseteq A$, then $X \rightarrow \subseteq W \rightarrow$. (Likewise if $V \subseteq Y \subseteq B$, then $Y \leftarrow \subseteq V \leftarrow$.)

**Solution**
Suppose $b \in X \rightarrow$. Then $x R b$ for all $x \in X$. Since $W \subseteq X$, we see that $x R b$ for all $x \in W$. This means that $b \in W \rightarrow$. Therefore, $X \rightarrow \subseteq W \rightarrow$. The statement in parentheses follows by a similar argument, with $A$ and $B$ interchanged.

**Problem 64.**
Prove that if $X \subseteq A$, then $X \subseteq X \rightarrow \leftarrow$. (Likewise if $Y \subseteq B$, then $Y \subseteq Y \leftarrow \rightarrow$.)

**Solution**
Let $u \in X$. Consider any $b \in X \rightarrow$. Then $x R b$ for all $x \in X$. So, in particular, $u R b$. Since $b$ was chosen arbitrarily in $X \rightarrow$, we see that $u R b$ for all $b \in X \rightarrow$. This entails that $u \in X \rightarrow \leftarrow$. Therefore $X \subseteq X \rightarrow \leftarrow$. The statement in parentheses follows by a similar argument.

**Problem 65.**
Prove that $X \rightarrow \leftarrow = X \rightarrow$ for all $X \subseteq A$ (and likewise $Y \leftarrow \rightarrow \leftarrow = Y \leftarrow$ for all $Y \subseteq B$).

**Solution**
By the Problem 64 we know that $X \subseteq X \rightarrow \leftarrow$. Applying Problem 63 to this inclusion yields

\[ X \rightarrow \leftarrow \subseteq X \rightarrow \]

On the other hand, from the parenthetical part of Problem 64 (with $Y = X \rightarrow$), we see that

\[ X \rightarrow \subseteq X \rightarrow \leftarrow \rightarrow \]

Combining these inclusion, we obtain $X \rightarrow = X \rightarrow \leftarrow \rightarrow$. The statement in parentheses follows by a similar argument.
Problem 67.
Let $A = B = \{ q \mid 0 < q < 1 \text{ and } q \text{ is rational} \}$. Let $R$ be the usual ordering on this set. Identify the system of closed sets. How are they ordered with respect to inclusion?

Solution
The closed subsets of $B$ are those of the form $X^- = \{ q \mid x \leq q \text{ for all } x \in X \}$, where $X$ can be any set of rationals properly between 0 and 1. Let $\mathcal{C}$ denote this collection. Such sets must be closed upward—that is if $q$ belongs and $q \leq r < 1$, where $r$ is rational, then $r$ must belong as well. This means that if $X^-$ has a least element $b$, then $X^- = \{ q \mid b \leq q < 1 \text{ and } q \text{ is rational} \}$. Consider the case when $X^-$ has no least element. This will happen if $X = \emptyset$, in which case $X^- = \emptyset^- = \{ q \mid 0 < q < 1 \text{ and } q \text{ is rational} \}$. But $X^-$ may fail to have a least element when $X$ is nonempty. In such a case, for every positive rational $r$ which is a lower bound of $X^-$ there must be $q \in X$ with $r < q$ (otherwise $r$ would be the least element of $X^-$).

Now suppose $X^-$ is not equal to $U^-$. Without loss of generality, pick $q \in X^-$ such that $q \notin U^-$. Since $U^-$ is closed upward, it must be that $q$ is a lower bound of $U^-$ since the rationals are linearly ordered. This means that $U^- \subseteq \{ r \mid q < r < 1 \text{ and } r \text{ is rational} \} \subseteq X^-$. The last inclusion holds since $X^-$ is closed upward. In this way, we see that $\mathcal{C}$ is linearly ordered by inclusion.

This linear ordering has a largest element, namely $\emptyset^- = \{ q \mid 0 < q < 1 \text{ and } q \text{ is rational} \}$. It also has a smallest element, namely $\{ q \mid 0 < q < 1 \text{ and } q \text{ is rational} \}^- = \emptyset$. Also, there is copy of the ordered set of rationals properly between 0 and 1 which sits densely in $\mathcal{C}$—notice $\{ r \}^- = \{ q \mid r \leq q < 1 \text{ and } q \text{ is rational} \}$ for every rational $r$ with $0 < r < 1$. (The industrious graudate student who has not done this should establish this density result.)

It follows that $(\mathcal{C}, \subseteq)$ must be isomorphic to the unit interval. The idea of this construction of the reals from the rationals traces back to Eudoxus, a contemporary of Socrates, and is usually called the Dedekind-MacNielle Completion.
Problem 68.
Let $E$ and $F$ be fields. Prove that $E$ 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 $E$ which fixes each element of $F$.

Solution

($\Rightarrow$)
Since $E$ is the algebraic closure of $F$ we know it is an algebraic extension of $F$. Let $K$ be an algebraic extension of $F$ and let $A$ be an algebraic closure of $K$. This means that $A$ is a algebraic extension of $K$ and that $A$ is algebraically closed. Since an algebraic extension of an algebraic extension is an algebraic extension, we find that $A$ is also an algebraic extension of $F$. Thus, $A$ is also an algebraic closure of $F$. We proved that any two algebraic closures of $F$ are isomorphic (via an isomorphism that fixes each element of $F$). So $A$ and $E$ are isomorphic. Take an isomorphism from $A$ onto $E$ and restrict it to $K$. This restriction is the desired embedding.

($\Leftarrow$)
We need to show that $E$ is algebraically closed, since we are given already that $E$ is an algebraic extension of $F$. So let $f(x) \in E[x]$. Extend $E$ to $E[r]$ by adjoining a root $r$ of $f(x)$, as Kronecker taught us to do. Then $E[r]$ is an algebraic extension of $E$. Therefore it is also an algebraic extension of $F$. Let $g(x) \in F[x]$ be the minimal polynomial of $r$. Let $K$ be a splitting field of $g(x)$. Now $K$ embeds into $E$ via a map which fixes each element of $F$. So $E$ contains a splitting field of $g(x)$. But $f(x) \mid g(x)$ in $E[x]$. So $f(x)$ must also split over $E$. Hence, $E$ is algebraically closed.

Problem 69.
Prove that if $E$ extends the field $F$ and $[E : F] = 2$, then $E$ is a normal extension of $F$.

Solution

We need to show that if the irreducible $f(x) \in F[x]$ has a root in $E$ then $f(x)$ splits in $E[x]$. So suppose $r \in E$ is a root of $f(x)$. Now, $f(x) = (x - r)g(x)$ for some $g(x) \in E[x]$. Since $f(x)$ is irreducible, we know that $[F[r] : F] = \deg f(x)$. But also that $2 = [E : F] = [E : F[r]][F[r] : F]$. So $\deg f(x)$ is either 1 or 2. So the degree of $g(x)$ is either 1 or 0. And we see that $f(x)$ splits in $E[x]$.

Problem 70.
Let $E$ be a field extending the field $F$. Let $L$ and $M$ be intermediate fields such that $L$ is the splitting field of a separable polynomial in $F[x]$. Let $L \lor M$ denote the smallest subfield of $E$ that extends both $L$ and $M$. Prove that $L \lor M$ is a finite normal separable extension of $M$ and that $\text{Aut}_M(L \lor M) \cong \text{Aut}_{M \lor L} L$.

Solution

Pick a separable $f(x) \in F[x]$ so that $L$ is a splitting field of $f(x)$ over $F$. Then $L$ is a splitting field of $f(x)$ over $L \cap M$ and $f(x)$ is still separable over $L \cap M$. By the Primitive Element Theorem, pick $u \in L$ so that $L = (L \cap M)[u]$. Evidently, $L \lor M = M[u]$ and $L \lor M$ is a splitting field of $f(x)$ over $M$. This means that $L \lor M$ is a finite normal separable extension of $M$. 

Solutions to Algebra Homework, Edition 19
17 March 2011
Next notice that every automorphism $\sigma$ of $L \lor M$ which fixes each element of $M$ is determined by what it does to the input $u$. Also notice that every such automorphism must take $u$ to a root of $f(x)$. So such an image of $u$ must belong to $L$, which is a splitting field of $f(x)$. Now each element of $L$ can be expressed as a linear combination of powers of $u$ using scalars from $L \cap M$. It follows that the image under $\sigma$ of any element of $L$ must again be an element of $L$. Hence, the restriction of $\sigma$ to $L$ is an automorphism of $L$ that fixes each element of $L \cap M$. It is easy to check (and the diligent graduate student will do the checking) that functional restriction is a homomorphism from the group $\text{Aut}_M(L \lor M)$ into $\text{Aut}_{L \cap M} L$. A short reflection on the kernel of this restriction map also reveals that the map is one-to-one.

The only part that remains is to show that the restriction map is surjective. So let $\tau$ be an automorphism of $L$ that fixes each element of $L \cap M$. The map $\tau$ is determined by the image of $u$. So let $\tau(u) = v$. We suppose $u \neq v$, since otherwise $\tau$ is just the identity map. Now the minimal polynomials of $u$ and $v$ over $L \cap M$ must be the same, say $g(x)$ and $g(x) \mid f(x)$. Since $u, v \in L$ and neither is a fixed point of $\tau$, we see that neither $u$ nor $v$ can be in $M$. Now let $h(x)$ be the minimal polynomial of $u$ over $M$. So all the coefficients of $h(x)$ lie in $M$. Now $h(x)$ splits in $L \lor M$, so $h(x) = (x-u)(x-u_1) \cdots (x-u_{m-1})$, where each of the $u_k$’s is an image of $u$ under some automorphism in $\text{Aut}_M(L \lor M)$. Since the images of $u$ all belong to $L$, we see that the coefficients of $h(x)$ also belong to $L$. But that means the also belong to $L \cap M$. Since $L \cap M \subseteq M$ and $h(x)$ is irreducible over $M$, we find that $h(x)$ is irreducible over $L \cap M$. This means that $h(x) = g(x)$ and that $v$ is one of the $u_k$’s. Hence there is an $\sigma \in \text{Aut}_M(L \lor M)$ such that $\sigma(u) = v$. Hence $\tau$ is the restriction to $L$ of $\sigma$. This means the restriction map is surjective.

**Problem 71.**
Let $L$ and $M$ be fields. Then the collection of functions from $L$ into $M$ can be regarded as a vector space over $M$. (Add functions like we do in calculus...). Prove that the collection of field embeddings from $L$ into $M$ is a linearly independent set in this vector space.

**Solution**
Suppose the collection of embeddings is not linearly independent. Then some finite collection of embeddings is not linearly independent. Among such finite collections, there must be some of least size. Pick one of these. Say it has size $n$ and that its members of the distinct embeddings $\lambda_0, \ldots, \lambda_{n-1}$. Pick $a_0, \ldots, a_{n-1} \in M$, with none of them $0$, so that

$$a_0 \lambda_0(x) + a_1 \lambda_1(x) + \cdots + a_{n-1} \lambda_{n-1}(x) = 0,$$

for all $x \in L$. It is evident that $n \geq 2$. So pick $u \in L$ so that $\lambda_0(u) \neq \lambda_1(u)$. Now notice

$$a_0 \lambda_0(u x) + a_1 \lambda_1(u x) + \cdots + a_{n-1} \lambda_{n-1}(u x) = 0,$$

for all $x \in L$. This in turn gives

$$a_0 \lambda_0(u) \lambda_0(x) + a_1 \lambda_1(u) \lambda_1(x) + \cdots + a_{n-1} \lambda_{n-1}(u) \lambda_{n-1}(x) = 0.$$

On the other hand, multiplying the very first displayed equation by $\lambda_0(u)$ we get

$$a_0 \lambda_0(u) \lambda_0(x) + a_1 \lambda_0(u) \lambda_1(x) + \cdots + a_{n-1} \lambda_0(u) \lambda_{n-1}(x) = 0.$$

Now, subtract the last two displayed equations to obtain

$$a_1 (\lambda_1(u) - \lambda_0(u)) \lambda_1(x) + \cdots + a_{n-1} (\lambda_{n-1}(u) - \lambda_0(u)) \lambda_{n-1}(x) = 0.$$

This shows that $\lambda_1, \ldots, \lambda_{n-1}$ are linearly dependent, violating the minimality of the original choice of the $\lambda$’s.
Problem 72.
Let $F$ be a field. We use $F^\times$ to denote the group of nonzero elements of $F$ under multiplication and the formation of multiplicative inverses. Show that every finite subgroup of $F^\times$ is a cyclic group.

Solution
Let $G$ be a finite subgroup of $F^\times$. Now $G$ is a finite Abelian group. So we know that $G$ is the direct sum of its Sylow subgroups. This means that it is enough to show the each nontrivial Sylow $p$-subgroup is cyclic. This means that it suffices to assume from the beginning that $G$ is a finite $p$-group. Let $b \in G$ be an element of maximal order, say $m = p^k$. The $1, b, b^2, \ldots, b^{m-1}$ are $m$ distinct roots of the polynomial $x^m - 1 \in F[x]$. This polynomial can have no other roots in $F$. Now let $c \in G$. The order of $c$ must be a power of $p$, say it is $p^\ell$. Then $\ell \leq k$ by the choice of $k$. Therefore the order of $c$ is a divisor of $m$. This means that $c^m = 1$. Hence $c$ is a root of $x^m - 1$. So $c$ must be among the powers of $b$. This means that $b$ generates $G$ and that $G$ is a cyclic group.

Problem 73.
Let $p$ be prime and let $H$ be a subgroup of $S_p$. Prove that if $H$ has a transposition and an element of order $p$, then $H = S_p$. Provide an explicit counterexample when $p$ is not prime.

Solution
Let the $p$-element set to be permutated be $\{0, 1, 2, \ldots, p-1\}$. Without loss of generality, suppose $(0, 1) \in H$. Now any element of $S_p$ of order $p$ must be a $p$-cycle. Let $\tau$ be a $p$-cycle. Observe that it is always possible to pick $k$ so that $\tau^k(0) = 1$. So without loss of generality, we can assume that $(0, 1, 2, \ldots, p-1) \in H$. Since we know that every permutation is a product of transpositions, it will suffice to show that every transposition can be generated by $(0, 1)$ and $(0, 1, 2, \ldots, p-1)$. Let us denote this $p$-cycle by $\tau$. The following contentions are easy to establish by direct calculation.

Contention: $\tau(j, k)\tau^{-1} = (j + 1, k + 1)$ where the $+$ works modulo $p$ and $j \neq k$.

Contention: $(j, \ell)(j, k)(j, \ell) = (\ell, k)$ where $j, k,$ and $\ell$ are distinct.

Contention: $\tau^\ell(j, k)\tau^{-\ell} = (j + \ell, k + \ell)$ where the $+$ works modulo $p$ and $j \neq k$.

According to the first two contentions, $(0, 1)$ and $\tau$ generate all transpositions of the form $(0, j)$. The last contention produces all the rest of the transpositions.

The contentions above hold, even if $p$ is not prime. What breaks down in the composite case, is that $\tau^k$ need not be a $p$-cycle when $0 < k < p$. As a result we have no justification for assuming the given transposition transposes adjacent elements of the longer cycle.

Here is a counterexample for $S_4$. Let $\tau = (0, 1, 2, 3)$ be the $4$-cycle and take $\sigma = (0, 2)$ as the transposition. Let $\gamma = (1, 3)$. We see that $\gamma = \tau \sigma \tau^{-1}$. We also see $\sigma = \tau \gamma \tau^{-1}$. We note, as well, that $\sigma$ and $\gamma$ are disjoint transpositions. This leads us to the following equations:

$\sigma \gamma = \gamma \sigma$
$\tau \sigma = \gamma \tau$
$\tau \gamma = \sigma \tau$
A direct calculation gives us
\[ \sigma \gamma = \tau^2 \]
Recalling that \( \tau \) has order 4 and transpositions have order 2, this leads us to the conclusion that the following 12 elements constitute a subgroup of \( S_4 \):
\[
\tau^0, \tau^1, \tau^2, \tau^3 \\
\sigma, \sigma \tau^1, \sigma \tau^2, \sigma \tau^3 \\
\gamma, \gamma \tau^1, \gamma \tau^2, \gamma \tau^3
\]
But \( S_4 \) has 24 elements, so the subgroup generated by \((0,2)\) and \((0,1,2,3)\) is a proper subgroup.

**Problem 74.**
Prove that \( x^5 - 2x^3 - 8x + 2 \) is not solvable by radicals over the field \( \mathbb{Q} \) of rational numbers.

**Solution**
Observe that this polynomial is irreducible according to Eisenstein and a Calculus I exercise shows that its derivative is 0 at \( \pm \sqrt{2} \). It follows that the polynomial has three real roots, one less than \( -\sqrt{2} \), one properly between \( -\sqrt{2} \) and \( \sqrt{2} \), and one greater than \( \sqrt{2} \). The remaining roots must be nonreal complex numbers and, since the polynomial has real coefficients, these remaining roots must be complex conjugates. By a Fact proven in class, the Galois group of the polynomial must be \( S_5 \) (since 5 is prime). Since \( 5 > 4 \) we know that this group is not solvable. So by Galois’ Criterion, the polynomial is not solvable by radicals.

**Problem 75.**
Let \( F \) be a finite field. Prove that the product of all the nonzero elements of \( F \) is \(-1\). Using this, prove Wilson’s Theorem:
\[(p-1)! \equiv -1 \pmod{p}\]
for every prime number \( p \).

**Solution**
Let \( q \) be the cardinality of \( F \). We know that the elements of \( F \) are precisely the roots of \( x^q - x \). This means that the roots of \( x^{q-1} - 1 \) are precisely the nonzero elements of \( F \). Let the nonzero elements be \( r_0, r_1, \ldots, r_{q-2} \). Then \( x^{q-1} - 1 = (x - r_0)(x - r_1)\ldots(x - r_{q-2}) \). This tells us that \(-1\) is the product of the nonzero elements of \( F \). (The careful graduate student will realize that \((-1)^{q-1} = 1\) for all possible values of \( q \).)

For the last bit, let \( F = \mathbb{Z}_p \) where \( p \) is prime. The nonzero elements of this field are \( 1, 2, 3, \ldots, p-1 \). Multiplication in \( \mathbb{Z}_p \) is performed by forming the product in \( \mathbb{Z} \) and then extracting the residue modulo \( p \). In other words, Wilson’s Theorem.
Problem 76.
Let \( E \) be the splitting field of \( x^5 - 2 \) over the field \( \mathbb{Q} \) of rationals. Find the lattice (draw a picture) of all fields intermediate between \( \mathbb{Q} \) and \( E \).

Solution
Let \( \zeta \) be a primitive 5th root of unity. Clearly, both \( \sqrt[5]{2} \) (the real fifth root of 2) and \( \sqrt[5]{2} \zeta \) are roots of \( x^5 - 2 \). So they belong to the splitting field \( E \). Dividing, we see that \( \zeta \in E \). It is evident that \( \sqrt[5]{2}, \sqrt[5]{2} \zeta, \sqrt[5]{2} \zeta^2, \sqrt[5]{2} \zeta^3, \sqrt[5]{2} \zeta^4 \) lists the five distinct roots of \( x^5 - 2 \). So \( E = \mathbb{Q} [\sqrt[5]{2}, \zeta] \).

To conserve notation we put
\[
    r_k := \sqrt[5]{2} \zeta^k \quad \text{for} \ 0 \leq k < 5
\]

So \( r_0, r_1, r_2, r_3, \) and \( r_4 \) are the five distinct roots of \( x^5 - 2 \) in \( E \).

Observe that \( [\mathbb{Q} [r_0] : \mathbb{Q}] = 5 \) since \( x^5 - 2 \) is irreducible over \( \mathbb{Q} \) by Eisenstein. Also observe that \( [\mathbb{Q} [\zeta] : \mathbb{Q}] = 4 \) since \( \zeta \) is a root of \( \lambda_5(x) \) which we know is irreducible over \( \mathbb{Q} \) and has degree 4. Thus \( [E : \mathbb{Q}] \) is divisible by both 5 and 4. This means \( [E : \mathbb{Q}] \) is divisible by 20, since 4 and 5 are relatively prime. Now consider \( [E : \mathbb{Q} [r_0]] \). Since \( \zeta \) is a root of \( \lambda_5(x) \), which has degree 4, we see that this dimension is no greater than 4. This means that \( [E : \mathbb{Q}] \) is no larger than 20. So we find that \( [E : \mathbb{Q}] = 20 \). It follows that \( [\mathbb{Q} [\zeta, r_0] : \mathbb{Q} [r_0]] = 4 \). In turn, this entails that \( \lambda_5(x) \) is irreducible over \( \mathbb{Q} [r_0] \). We also get \( [E : \mathbb{Q} [\zeta]] = 5 \). Since \( E = \mathbb{Q} [r_0, \zeta] \) and \( r_0 \) is a root of the monic polynomial \( x^5 - 2 \), we see \( x^5 - 2 \) is irreducible over \( \mathbb{Q} [\zeta] \).

Here are four obvious intermediate fields: \( \mathbb{Q}, \mathbb{Q} [\zeta], \mathbb{Q} [r_0] \) and \( E = \mathbb{Q} [\zeta, r_0] \). It is easy to see that these are all distinct. Clearly any field properly between \( \mathbb{Q} \) and \( E \) must have dimension 2, 4, 5, or 10. So the only remaining question is whether there are any others. There are.

Since \( x^5 - 2 \) is irreducible over \( \mathbb{Q} \) (by Eisenstein) Kronecker tells us that \( \mathbb{Q} [r_k] \) is a subfield of \( E \) of dimension 5, when \( 0 \leq k < 5 \). No two of these fields can coincide, since given both \( r_i = \sqrt[5]{2} \zeta^i \) and \( r_j = \sqrt[5]{2} \zeta^j \) with \( i \neq j \), after a bit of fiddling we can get both \( r_0 \) and \( \zeta \) using just the field operations. So now we have at least five intermediate fields of dimension 5.

Now \( \mathbb{Q} [\zeta] \) is the splitting field of the cyclotomic polynomial \( \lambda_5(x) \) over \( \mathbb{Q} \). This polynomial is irreducible over \( \mathbb{Q} \) and has degree 4. So Kronecker tells us that it has dimension 4. So its Galois group has order 4. Kronecker also told us that the map that sends \( \zeta \mapsto \zeta^2 \) extends to a automorphism of \( \mathbb{Q} [\zeta] \). This automorphism belongs to the Galois group and the automorphism is easily seen to have order 4. So the Galois group is the cyclic group of order 4. The subgroup lattice of this group is a three-element chain. By the Fundamental Theorem of Galois Theory, there will be exactly one field of dimension 2 sitting between \( \mathbb{Q} \) and \( \mathbb{Q} [\zeta] \). We know that conjugation, restricted to \( \mathbb{Q} [\zeta] \) is the element of order 2. The field sitting properly between \( \mathbb{Q} \) and \( \mathbb{Q} [\zeta] \) is the fixed field of conjugation. Notice that \( \zeta + \zeta^4 = \zeta + \bar{\zeta} \not\in \mathbb{Q} \), for otherwise \( (x - \zeta)(x - \bar{\zeta}) \in \mathbb{Q}[x] \) and it would be a factor of the irreducible polynomial \( \lambda_5(x) \). But \( \zeta + \bar{\zeta} \) is obviously fixed by conjugation. So, taking \( \omega = \zeta + \bar{\zeta} \) we find the field of dimension 2 is \( \mathbb{Q} [\omega] \). For reassurance, we note that \( x^2 + x - 1 \) is the minimal polynomial of \( \omega \).

Now let \( r \) be one of our five distinct roots of \( x^5 - 2 \). Since \( \mathbb{Q} [r] \) has dimension 5 it follows that any irreducible polynomial in \( \mathbb{Q}[x] \) of degree 2 (or 3) will also be irreducible over \( \mathbb{Q} [r] \). By Kronecker, this means that \( \mathbb{Q} [r, \omega] \) must have dimension 10 over \( \mathbb{Q} \).

At this point, we have one field of dimension 1 (namely \( \mathbb{Q} \)), one field of dimension 2, one field of dimension 4, five fields of dimension 5, five fields of dimension 10 and one field of dimension 20.

Here is what the diagram looks like up to this point.
Can there be any other intermediate fields?

Let’s invoke the Fundamental Theorem of Galois Theory. The Galois group \( \text{Gal}(E/\mathbb{Q}) \) has cardinality 20 and it is embeddable into \( S_5 \). Here the underlying 5-element set is our five distinct roots of \( x^5 - 2 \). Notice that \( \text{Gal}(E/\mathbb{Q}[r_0]) \) is a subgroup of \( \text{Gal}(E/\mathbb{Q}) \). But \( \text{Gal}(E/\mathbb{Q}[r_0]) \) is a cyclic group of order 4—the reasoning we used for \( \text{Gal}([\zeta]/\mathbb{Q}) \) works here too. This means there is a 4-cycle permuting the nonreal roots. The uniqueness of splitting fields argument also gives us an automorphism of \( E \) that sends \( r_0 \mapsto r_1 \) which fixes \( \zeta \). This automorphism has order 5. So in \( \text{Gal}(E/\mathbb{Q}) \) we have a 4-cycle and a 5-cycle. If you play around a bit, you will see that this generates a subgroup of order 20. After a while you can churn out all the subgroups and discover there are not more intermediate fields. There are even software programs for carrying out these kinds of group calculations.

A more sophisticated approach would find that there is one Sylow 5-subgroup and 5 Sylow 2-subgroups. In fact, Sylow tells us there are either 5 Sylow 2-subgroups or just 1. Certainly, there are no more. Since we already must have at least 5, Sylow tells us we have exactly 5. The Sylow 2-subgroups are all conjugate and so are isomorphic. Since we have an element of order 4, it follows that they are all copies of the cyclic group of order 4 and each has exactly one subgroup of order 2. Since every 2-subgroup is included in a Sylow 2-subgroup, we see that there are no more than 5 subgroups of order 2. But by our field analysis above, there are at least 5. We have in hand all possible subgroups, except those of order 10. A subgroup of order 10 must include the only subgroup of order 5 and it must have an element of order 2. There are exactly 5 elements of order 2. One of them is complex conjugation. Restricted to our 5 roots, it is the permutation \( \sigma = (r_1, r_4)(r_2, r_3) \). Let \( \tau = (r_0, r_1, r_2, r_3, r_4) \). An easy calculation shows

\[ \sigma \tau^4 = \tau \sigma. \]

By way of this equation, any product of \( \sigma \)'s and \( \tau \)'s in any order can be rearranged to obtain an element on the list of 10 distinct permutations below:

\[ \tau^0, \tau, \tau^2, \tau^3, \tau^4, \sigma, \sigma \tau, \sigma \tau^2, \sigma \tau^3, \sigma \tau^4. \]
These elements comprise a subgroup of order 10. We would be done, if we can show that $\sigma \tau^k$ has order 2 for $0 \leq k < 5$, since then the subgroup has all the elements of order 5 as well as all the elements of order 2. Straightforward calculations show

$$
\sigma = (r_1, r_4)(r_2, r_3) \\
\sigma \tau = (r_0, r_4)(r_1, r_3) \\
\sigma \tau^2 = (r_0, r_3)(r_1, r_2) \\
\sigma \tau^3 = (r_0, r_2)(r_3, r_4) \\
\sigma \tau^4 = (r_0, r_1)(r_2, r_4)
$$

and these all have order 2. So we have found the unique subgroup of order 10. So our lattice diagram above accounts for all the intermediate fields.

**Problem 77.**

Let $F$ be a field of characteristic $p$, where $p$ is a prime. Let $E$ be a field extending $F$. Prove that $E$ 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 $a \in F$.

**Solution**

($\Leftarrow$)

Observe that $f(x) = x^p - x - a$ is a function with period 1. That is

$$f(x + 1) = (x + 1)^p - (x + 1) - a = x^p + 1^p - x - 1 - a = x^p - x - a = f(x).$$

So if $u \in E$ is a root of $f(x)$ then all of $u, u+1, u+2, \ldots, u+p-1$ are also roots and they are all distinct. This means that every root of $f(x)$ is really a primitive root of $f(x)$. So $E = F[u]$ where $u$ is any root of $f(x)$. Since we are assuming that $f(x)$ is irreducible, Kronecker tells us that $[E : F] = \deg f(x) = p$. So all our desires are fulfilled by the Key Theorem.

($\Rightarrow$)

Now we assume that $E$ is a normal separable extension of $F$ of dimension $p$ over $F$. By the Key Theorem $E$ is the splitting field of some separable polynomial over $F$ and the Galois group $\text{Gal}(E/F)$ is a cyclic group of cardinality $p$. Let $\text{Id}, \sigma, \ldots, \sigma^{p-1}$ be the elements of this Galois group. Problem 8 tells us that, as members of a vector space over $E$ these maps are linearly independent. Hence

$$u + \sigma(u) + \sigma^2(u) + \cdots + \sigma^{p-1}(u)$$

cannot be 0 for every $u \in E$. So pick $u \in E$ so that

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

Now notice that $\sigma(b) = \sigma(u) + \sigma^2(u) + \cdots + \sigma^{p-1}(u) + \sigma^p(u) = b$ since $\sigma$ has order $p$. So $b$ is fixed by each element of the Galois group. By the Fundamental Theorem of Galois Theory, $b \in F$. Now let

$$c = \sigma(u) + 2\sigma^2(u) + \cdots + (p-1)\sigma^{p-1}(u).$$
Then
\[ \sigma(c) = \sigma^2(u) + 2\sigma^3(u) + \cdots + (p-2)\sigma^{p-1}(u) + (p-1)\sigma^p(u) \]
\[ = \sigma^2(u) + 2\sigma^3(u) + \cdots + (p-2)\sigma^{p-1}(u) + (p-1)u \]
\[ = \sigma^2(u) + 2\sigma^3(u) + \cdots + (p-2)\sigma^{p-1}(u) + (-1)(b - \sigma(u) - \sigma^2(u) - \cdots - \sigma^{p-1}(u)) \]
\[ = \sigma(u) + 2\sigma^2(u) + \cdots + (p-1)\sigma^{p-1}(u) - b \]
\[ = c - b \]

Now put \( v = -\frac{c}{b} \). From this we see
\[ \sigma(v) = \frac{\sigma(c)}{\sigma(b)} = \frac{c - b}{b} = \frac{c}{b} + 1 = v + 1. \]

So, more generally, we see that \( \sigma^k(v) = v + k \) for all natural numbers \( k < p \).

Now put \( a = v^p - v \). Observe
\[ \sigma(a) = (\sigma(v))^p - \sigma(v) = (v+1)^p - (v+1) = v^p + 1^p - v - 1 = v^p - v = a. \]

This means that \( a \) is fixed by all the members of the Galois group. So \( a \in F \), since \( F \) is the fixed field of the Galois group. That is \( v \) is a root of \( x^p - x - a \in F[x] \). Since the members of the Galois group fix the elements of \( F \), the image of \( v \) under any one of these members must also be a root of \( x^p - x - a \). So each \( (x-(v+k)) \) is a factor of \( x^p - x - a \). It is not too hard to see that \( x^p - x - a = \prod_{k<p} (x-(v+k)) \).

If we could show that \( x^p - x - a \) is irreducible, then Kronecker would tell us that \( [F[v]:F] = p = [E:F] \). So \( E = F[v] \) and we would be done.

Now the minimal polynomial (over \( F \)) of \( v \) has degree \( [F[v]:F] \). Since \( F[v] = F[v+k] \) we see that the minimal polynomial of \( v \) and the minimal polynomial of \( v+k \) (for any \( k < p \)) have the same degree. Also these minimal polynomials are factors of \( x^p - x - a \) and, in fact, must give the decomposition of \( x^p - x - a \) into its irreducible factors. So the common degree of the minimal polynomials must itself be a factor of the prime \( p \). So either \( x^p - x - a \) is irreducible or else all those minimal polynomials have degree 1. In the latter case, \( v \in F \). This is impossible since \( \sigma(v) = v+1 \neq v \), meaning that \( v \) is not fixed by \( \sigma \) and so cannot belong to the fixed field \( F \).

---

**Solutions to Algebra Homework, Edition 21**

31 March 2011

**Problem 78.**

Let \( E \) be a finite separable extension of the field \( F \). Prove that the trace maps \( E \) onto \( F \).

**Solution**

Suppose first that \( E \) is a Galois extension of \( F \). Let \( G = \text{Gal}(E/F) \). The trace is the map \( T : E \to F \) defined by
\[ T(u) = \sum_{\eta \in G} \eta(u). \]

We know the trace is a linear functional. So the image of \( E \) under the trace must be a subspace of the one-dimensional space \( F \). This means the only choices for the image of \( E \) under the trace are \( \{0\} \) and
by Problem 8, we know that the elements of the Galois group are linearly independent. This means that

\[ T = \sum_{\eta \in G} 1\eta \]

cannot be the zero map, since the coefficients in this linear combination (all 1's) are not all 0. So there must be \( u \in E \) with \( T(u) \neq 0 \). Hence, the image of \( E \) under \( T \) cannot be \( \{0\} \) and so it must be \( F \).

What if \( E \) is not a Galois extension of \( F \)? Then there is a cheap way to answer the question and a more expensive way. The cheap way is to say that all we need to prove is that for every \( a \in F \) there is \( u \in E \) so that \( T(u) = a \). All we need to do is let \( F' \) be the fixed field of \( G \). Then \( T \) maps \( E \) into \( F' \) since

\[ \sigma(T(u)) = \sum_{\eta \in G} (\sigma \circ \eta)(u) = \sum_{\eta \in G} \eta(u) = T(u), \]

for all \( \sigma \in G \). This shows that \( T(u) \) belongs to the fixed field of \( G \), namely \( F' \). Then the argument above shows that \( T \) maps \( E \) onto \( F' \) and hence onto \( F \).

The more expensive way actually addresses a slightly different question. Namely, suppose \( F \leq E \leq K \) where \( K \) is a finite Galois extension of \( F \). Then the restriction of the trace of \( K \) over \( F \) to \( E \) is a linear functional that maps \( E \) onto \( F \). Roughly speaking, in a Galois extension the trace of an element is a certain multiple of the sum of roots of its minimal polynomial over \( F \). In a Galois extension any irreducible polynomial which has a root actually splits so the full complement of roots is available. It is easy to see that this sum of roots is, essentially, the coefficient of \( x^{n-1} \) in the minimal polynomial, where \( n \) is the degree of the minimal polynomial. So we see it is in \( F' \).

Here is the beginning of what needs to be done. Let \( T : K \to F \) be the trace. So for \( u \in E \)

\[ T(u) = \sum_{\eta \in G} \eta(u). \]

Now each \( \eta(u) \) is a root of the minimal polynomial of \( u \) and every root of the minimal polynomial must occur in this way (remember how we extended maps to get the uniqueness of the splitting fields?). So the idea is to regroup the sum above into packets that each include exactly one occurrence of each root. To prove that you can get away with this regrouping, with no terms left over, it is a good idea consider the subgroup \( H = \text{Gal} E/F[u] \). Use \( H \) to partition \( G \) into left cosets. Try showing first that the number of cosets is the same as the number of roots. Then each time you make up a packet take one permutation from each coset. Each time this decreases the sizes of the cosets. But the cosets all have the same size, so the whole process finishes cleanly. I leave the details in your hands.

There are actually several ways to define the trace. A good number of authors define the trace in separable extensions by essentially saying ‘Find the minimal polynomial of the element \( u \). Find all of its roots (in some splitting field) and add them up. That is virtually the trace of \( u \).” Another way is to observe that multiplication by \( u \) is a linear operator on \( E \) construed as a vector space over \( F \) and then to take the trace of \( u \) to be the linear algebra trace of this associated linear operator.

All these ways prove to be equivalent for Galois extensions.

**Problem 79.**

Let \( E \) be a finite extension of the finite field \( F \). Prove that both the norm and the trace map \( E \) onto \( F \).

**Solution**

Let us suppose that \( |F| = p^r = m \), where \( p \) is prime, and that \( |E| = q = p^r = m^n \) so that \( |E : F| = n \). Recall that \( E \) is the splitting field of \( x^n - x \), which is a separable polynomial, that the \( q \) distinct roots
of this polynomial are exactly the \( q \) elements of \( E \). So \( E \) is a Galois extension of \( F \) and we also know that it is a cyclic extension with the generator of the Galois group being the automorphism \( \eta \) such that \( \eta(u) = u^m \) for all \( u \in E \). (See Theorem 4.26 in Jacobson’s Basic Algebra I.)

We can refer to the problem above to handle the trace. Here there are no fine points, since we are dealing with a Galois extension.

We need to show that the norm \( N \) maps \( E \) onto \( F \). (We certainly know it maps \( E \) into \( F \), in case you were wondering). Since \( N(0) = 0 \), we need only concern ourselves with the two multiplicative groups \( E^\times \) and \( F^\times \) of nonzero elements. Both of these groups are cyclic and \( N \) restricted to \( E^\times \) is a homomorphism into \( F^\times \). Let \( a \) be a generator of \( E^\times \). So \( E = F[a] \).

We have, for any \( u \in E \),
\[
N(u) = u \cdot \eta(u) \cdot \eta^2(u) \cdots \eta^{n-1}(u) = u \cdot u^m \cdot u^{m^2} \cdots u^{m^{n-1}} = u^s \text{ where } s = \sum_{k<n} m^k.
\]
We know that \( s = \frac{m^n - 1}{m - 1} = \frac{q - 1}{m - 1} \). But \( a \in E^\times \) is an element of order \( q - 1 \). So \( a^s = N(a) \in F^\times \) must be an element of order \( m - 1 \). In other words, \( N(a) \) generates \( F^\times \). Therefore, \( N \) maps \( E \) onto \( F \).

---

**Problem 80.**

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

**Solution**

We do not lose generality by supposing that \( f(x) \) is monic. Factor \( f(x) \) into irreducibles over \( R[x] \):
\[
f(x) = (x - r_0) \cdots (x - r_{n-1})g_0(x) \cdots g_{m-1}(x)
\]
where the \( g_k(x) \) are monic irreducibles of degree 2.

There is an interesting fact about those monic irreducibles of degree 2. Completing the square gives
\[
g(x) = x^2 + bx + c = x^2 + bx + \frac{b^2}{4} + c - \frac{b^2}{4} = \left( x + \frac{b}{2} \right)^2 + \left( c - \frac{b^2}{4} \right)
\]
but since the difference of squares has been factorable since puberty, we see that \( -(c - \frac{b^2}{4}) \) must not be a square. Since in a real closed field, the positive elements and the nonzero squares coincide, we see that \( (c - \frac{b^2}{4}) \) must be positive. It follows that \( g(u) > 0 \) for all \( u \in R \).

Now \( f(a) f(b) < 0 \) is just a way of saying the \( f(a) \) and \( f(b) \) have opposite signs (and neither is 0). Let’s plug \( a \) and \( b \) into our factorization.
\[
0 > f(a) f(b) = [(a - r_0)(b - r_0)][(a - r_1)(b - r_1)] \cdots [(a - r_{n-1})(b - r_{n-1})]g_0(a)g_0(b) \cdots g_{m-1}(a)g_{m-1}(b)
\]
If all the bracketed pairs were positive we would get a contradiction since all those \( g \)’s evaluate positively. So some bracketed pair is negative. Say \( 0 > (a - r_0)(b - r_0) \). Since we have \( a < b \), this means that \( a < r_0 < b \).
Problem 81.
Let $R$ be a real closed field, let $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n = f(x) \in R[x]$, and put $M = |a_0| + |a_1| + \cdots + |a_{n-1}| + 1$. Prove that every root of $f(x)$ which belongs to $R$ belongs to the interval $[-M, M]$.

Solution
Let $r$ be a root of $f(x)$. If $|r| \leq 1$, the result is obvious. So suppose $|r| > 1$. Then
\[
0 = \frac{0}{r^{n-1}} = \frac{f(r)}{r^{n-1}} = \frac{a_0}{r^{n-1}} + \frac{a_1}{r^{n-2}} + \cdots + \frac{a_{n-1}}{r} + r.
\]
This gives us
\[
r = -\left[ \frac{a_0}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} \right].
\]
So $|r| = \left| \frac{a_0}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} \right| \leq \frac{|a_0|}{|r|^n} + \cdots + \frac{|a_{n-1}|}{|r|} \leq |a_0| + \cdots + |a_{n-1}| = M - 1 < M.$

In the above argument we used the triangle inequality and other properties of the ordering and the absolute value that are familiar from the ordering on the reals. The hard working graduate students will know these work in any ordered field.

Solutions to Algebra Homework, Editon 22
7 April 2011

Problem 82.
Prove that every element of a finite field can be written as the sum of two squares.

Solution
First observe that if $a = b^2$, then $a = b^2 + 0^2$ a sum of two squares. So, if you like, this phrases means ‘the sum of one or two squares’.

Now let $p$ be the characteristic of our finite field $F$ and let $q = p^k$ be the number of elements in our finite field. We know that $F$ is the splitting field (over $\mathbb{Z}_p$) of $x^q - x$. So every element of $F$ is a $q$th power of some element of $F$ (namely, itself). So if $p$ happens to be the even prime 2, then we see that every element of $F$ is a square and so is also the sum of two squares.

From this point we take $p$ to be an odd prime.

We know that the multiplicative group of nonzero elements of $F$ is cyclic. Let $a$ be a generator of this group. Then $F$ consists of 0 and the $q - 1$ powers $a^0, a^1, \ldots a^{q-2}$ of the generator $a$. The even powers of $a$ are squares, so they work out fine. We have to contend with the others. They look like $a^{2k+1} = (a^k)^2 a$. If we just knew that $a = b^2 + c^2$, then $a^{2k+1} = (a^k)^2 a = (a^k)^2 (b^2 + c^2) = (a^k b)^2 + (a^k c)^2$. This would finish the problem. So what we need is only to show that the generator $a$ is the sum of two squares.

Examining the list above we find at least 0, $a^0, a^2, \ldots, a^{q-3}$ (recall $q$ is odd so $q - 3$ is even). Counting these we find at least $1 + \frac{q-1}{2} = \frac{q+1}{2}$ squares. We want to find a square $b^2$ so that $a - b^2$ is also a square. We have at least $\frac{q+1}{2}$ elements of the form $a - b^2$ (since that is at least the number of squared elements that we already listed). Thus we know the set of squares accounts for more than half of the elements of $F$ and the set of elements of the form $a - b^2$ accounts for more than half the elements of $F$. Thus these two sets must share at least one element. This is just another way to say that $a - b^2 = c^2$ for appropriately chosen elements $b$ and $c$. That does it.
Problem 83.
Prove that every polynomial with rational coefficients whose splitting field over \( \mathbb{Q} \) has dimension 1225 is solvable by radicals.

Solution
Let \( E \) be the splitting field. We know that \( G = \text{Gal}(E/\mathbb{Q}) \) has 1225 elements. Now \( 1225 = 5^27^2 \). Let \( n_5 \) be the number of Sylow 5-subgroups of the Galois group and let \( n_7 \) be the number of Sylow 7-subgroups. We know

\[
\begin{align*}
n_5 &\equiv 1 \pmod{5} \\
n_5 &| 7^2 \\
n_7 &\equiv 1 \pmod{7} \\
n_7 &| 5^2
\end{align*}
\]

An examination of these constraints reveals that \( n_5 = 1 = n_7 \). Let \( N \) be the unique Sylow 5-subgroup and \( K \) be the unique Sylow 7 subgroup. We see that these must be normal subgroups since any conjugation is an automorphism. We see by Lagrange that \( N \) and \( K \) must have a trivial intersection since 25 and 49 are relatively prime. Finally, one those isomorphism theorems tells us

\[
NK/K \cong N/(N \cap K).
\]

This entails that \( |NK| = |N||K| = 5^27^2 = |G| \). So \( NK = G \), because \( G \) is finite. All this means that \( G \cong N \times K \).

Now the orders of \( N \) and \( K \) are squares of primes. This means that \( N \) and \( K \) are both Abelian. Since \( G \) is their direct product, we see that \( G \) is Abelian, as well. But every Abelian group is solvable, so \( G \) is solvable. By Galois’ Theorem, any polynomial with splitting field \( E \) must be solvable by radicals.

Problem 84.
Let \( F \) be a field. Prove that the following are equivalent.
(a) \( F \) is not algebraically closed but there is a finite upper bound on the degrees of the irreducible polynomials in \( F[x] \).
(b) \( F \) is a real closed field.

Solution
The upward direction is clear. If \( F \) is real closed, then \( x^2 + 1 \) has no solution in \( F \). Hence \( F \) not algebraically closed. On the other hand, \( F[\sqrt{-1}] \) is the algebraic closure of \( F \). It has dimension 2. So 2 is an upper bound on the degrees of irreducible polynomials in \( F[x] \).

Now suppose that \( F \) is not algebraically closed and there is an upper bound on the degrees of irreducible polynomials in \( F[x] \).

We first argue that \( F \) is perfect. Since every field of characteristic 0 is perfect we suppose that \( F \) has prime characteristic \( p \). So \( F \) is perfect if and only if every element of \( F \) is a \( p \)-th power. Suppose, for contradiction, that \( a \in F \) is not a \( p \)-th power. Then it is our contention that \( x^{pe} - a \) is irreducible for every natural number \( e \). Let \( E \) be a splitting field of \( x^{pe} - a \). Then in \( E[x] \) we have the factorization \( x^{pe} - a = (x - r)^{pe} \), where \( r^{pe} = a \in F \). Let \( g(x) \) be a irreducible monic factor of \( x^{pe} - a \) in \( E[x] \). So \( g(x) = (x-r)^k \) for some \( k \). So \( r^k \in F \). Let \( d \) be the greatest common divisor of \( k \) and \( p^e \) and pick integers \( a \) and \( b \) so that \( d = ak + bp^e \). The \( r^{pe} = (r^p)^b(r^k)^a \in F \). Now \( a = r^{pe} = (r^p)^{d} \).

Since \( a \) is not a \( p \)-th power, we conclude that \( e = d \). This means that \( g(x) = x^{pe} - a \) and we conclude that \( x^{pe} - a \) is irreducible. But this is impossible since there is a bound on the degrees of irreducible polynomials in \( F[x] \).
polynomials. So \( F \) is perfect. Notice this is the very same argument that was part of the proof of the Artin-Schreier Theorem given in class.

Let \( C \) be the algebraic closure of \( F \). Our plan is to prove that \( [C : F] \) is finite and then appeal to the Artin-Schreier Theorem. Let \( d \) be the largest amongst the degrees of irreducible polynomials in \( F[x] \). Let \( b \in C \) be a root of an irreducible polynomial of degree \( d \). So \( [F[b] : F] = d \). We contend that \( C = F[b] \). Since \( F[b] \subseteq C \) is clear, pick \( c \in C \). Then \( F[b,c] \) is a finite extension of \( F \) and since \( F \) is perfect, it is also a separable extension. So there is an element \( a \) such that \( F[b,c] = F[a] \). So we get \( d \geq [F[a] : F] = [F[b,c] : F[b]] [F[b] : F] = [F[b,c] : F[b]] d \geq d \), where the first inequality holds since \( [F[a] : F] \) is the degree of the minimal polynomial of \( a \) and \( d \) bounds such degrees. It follows that \( F[b,c] = F[b] \). So \( c \in F[b] \). Hence \( C = F[b] \) and \( [C : F] = d \), which is finite.

**Problem 85.**

Let \( E \) be the splitting field over \( \mathbb{Q} \) of \( x^4 - 2 \). Determined all the fields intermediate between \( E \) and \( \mathbb{Q} \). Draw a diagram of the lattice of intermediate fields.

**Solution**

Let \( r \) be the positive real fourth root of 2. Then the roots of \( x^4 - 2 \) are \( r, -r, ri, \) and \( -ri \). So \( E = \mathbb{Q}[r, i] \). Notice that \( [\mathbb{Q}[r] : \mathbb{Q}] = 4 \) by Kronecker since \( x^4 - 2 \) is irreducible over \( \mathbb{Q} \) by Eisenstein. For the same reason, \( [\mathbb{Q}[ri] : \mathbb{Q}] = 4 \). Since \( \mathbb{Q}[r] \) is contained in the reals, we see that \( i \notin \mathbb{Q}[r] \). So \( x^2 + 1 \) is irreducible over \( \mathbb{Q}[r] \). We obtain \( [\mathbb{Q}[r,i] : \mathbb{Q}[r]] = 2 \). Since \( E = \mathbb{Q}[r,i] \), we arrive at \( [E : \mathbb{Q}] = 8 \) and we also find \( [\mathbb{Q}[r,i] : \mathbb{Q}[ri]] = 2 \).

At this stage we have found the following fields: \( \mathbb{Q} \), at the bottom, \( E = \mathbb{Q}[r,i] \) at the top, \( \mathbb{Q}[r] \) and \( \mathbb{Q}[ri] \) somewhere in the middle (and these two fields are incomparable—which takes just a finger exercise), and \( \mathbb{Q}[i] \) which has dimension 2 over \( \mathbb{Q} \). Along these lines we find one more field: \( \mathbb{Q}[\sqrt{2}] \). This field has dimension 2 over \( \mathbb{Q} \) since \( x^2 - 2 \) is irreducible (by Eisenstein) and it is contained in both \( \mathbb{Q}[r] \) and \( \mathbb{Q}[ri] \) since \( r^2 = \sqrt{2} = -(ri)^2 \). This makes one more field visible—namely, \( \mathbb{Q}[\sqrt{2}, i] \).

Are there more subfields of \( E \)? Well, in \( E \) we have \( i \), which is a primitive fourth root of unity, and we have \( \sqrt{2} \). So we also have \( \frac{\sqrt{2}}{2} (1 + i) \) which is a fourth root of \(-1\) and also a primitive 8th root of unity. Surely this should get us more subfields. Indeed, a bit more fiddling shows that \( \frac{1}{\sqrt{2}} (1 + i) \) is a root of \( x^4 + 2 \) (which is irreducible over \( \mathbb{Q} \)) and the other three roots of this polynomial are \( -\frac{1}{\sqrt{2}} (1 + i), \frac{1}{\sqrt{2}} (1 - i), \) and \(-\frac{1}{\sqrt{2}} (1 - i) \). So it is clear that \( E \) is also the splitting field of \( x^4 + 2 \). This gets us two more intermediate fields, namely \( \mathbb{Q}[\frac{1}{\sqrt{2}} (1 + i)] \) and \( \mathbb{Q}[\frac{1}{\sqrt{2}} (1 - i)] \). To keep the notation simple let \( \omega = \frac{1}{\sqrt{2}} (1 + i) \). So its complex conjugate \( \bar{\omega} = \frac{1}{\sqrt{2}} (1 - i) \).

Let’s give drawing the lattice a stab.
We have done a fairly thorough job of showing the left side of this picture is correct—we even know that each of the coverings in this part represent extensions of dimension 2. The same kind of analysis shows that the right half of the picture works the same way. In particular, all the joins and meets in the picture are correct and all the coverings have dimension 2.

At this stage, what we know is that we have at least ten intermediate fields that constitute a sublattice of the lattice of all intermediate fields. We still have to wonder if we have them all.

To see that our diagram is complete, let us turn to the group side of the Galois connection. We know that the Galois group of $E$ over $\mathbb{Q}$ has order 8. Up to isomorphism, there are just 5 groups of order 8: the three Abelian groups $(\mathbb{Z}/2)^3$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_8$; as well as the dihedral group of order 8 and the group of quaternions. If we knew enough about finite groups, we would know that of these groups the only one which is embeddable into $S_4$ is the dihedral group and, moreover, the lattice of subgroups of this dihedral group is dually isomorphic to the lattice of fields we just drew. So this would finish our problem, since we cannot have more intermediate fields than we have subgroups.

What do we do if our background in small finite groups is weaker than the line of reasoning above would support?

Consider $\sigma \in \text{Gal}(E/\mathbb{Q})$. The automorphism $\sigma$ is completely determined by what it does to $r$ and $i$, since $E = \mathbb{Q}[r,i]$. Since $\sigma$ must carry roots of a polynomial in $\mathbb{Q}[x]$ to roots of the same polynomial, we see that $\sigma(i) \in \{i, -i\}$ and that $\sigma(r) \in \{r, -r, ri, -ri\}$. There are at most 2 ways to fulfill the first constraint and at most 4 ways to fulfill the second. But there must be altogether 8 such automorphisms. So in fact every one of these 8 choices leads to an automorphism. Let us let $\sigma$ be the automorphism that fixes $r$ and sends $i$ to $-i$. This is just complex conjugation restricted to $E$. Also let $\tau$ be the automorphism that fixes $i$ but sends $r$ to $ri$. Observe that $\tau^2(r) = \tau(ri) = \tau(r)i$ and $\tau(r)i = (ri)i = -r$. Then also $\tau^3(r) = \tau(-r) = -\tau(r) = -ri$. Of course, $\tau^4(r) = r$, making $\tau^4$ the identity map. So $\tau$ is an automorphism of order 4. Next, notice $\tau(\sigma(r)) = \tau(r) = ri$ while $\sigma(\tau(r)) = \sigma(r)i = -ri$. This means that $\tau \circ \sigma \neq \sigma \circ \tau$. So our Galois group is not Abelian. The same kind of calculation shows that $\sigma \circ \tau = \tau^3 \circ \sigma$.

It is routine to see that the eight members of the Galois group are: $\text{Id}$ (the identity map), $\tau, \tau^2, \tau^3, \sigma, \tau\sigma, \tau^2\sigma$, and $\tau^3\sigma$. $\tau$ and $\tau^3$ are both of order 4 (and generate the same subgroup). The elements of order 2 are $\tau^2, \sigma, \tau\sigma, \tau^2\sigma$, and $\tau^3\sigma$, and there are no elements of other orders. So the Galois group has exactly 5 subgroups of order 2, so there are exactly 5 subfields of codimension 2. These are the five fields across the top of our lattice diagram. What about subgroups of order 4? There is the cyclic subgroup (the one generated by $\tau$). The only other possibilities are the subgroups generated by selecting two different elements of order 2. Direct calculation shows that $\{\text{Id}, \sigma, \tau^2, \tau^2\sigma\}$ and $\{\text{Id}, \tau^2, \tau\sigma, \tau^3\sigma\}$ are indeed subgroups of order 4. In doing these calculations, it helps to use $\sigma \tau = \tau^3 \sigma$. This only leaves four more pairs to check:

\[
(\tau^2\sigma)(\tau^3\sigma) = \tau^3 \\
(\tau\sigma)(\sigma) = \tau \\
(\tau^3\sigma)(\sigma) = \tau^3 \\
(\tau\sigma)(\tau^2\sigma) = \tau^3
\]

so that each of these pairs generates more than four elements (and hence generates everything). So we wind up with exactly 3 subgroups of order 4. This means there are only 3 subfields of codimension 4. We have found everything.
Problem 86.
Prove that the field of real numbers has only one ordering that makes it into an ordered field. In
contrast, prove that $\mathbb{Q}[\sqrt{2}]$ has exactly two such orderings.

Solution
Any real closed field, including the field of real numbers, has a unique order. This is because, in a
real closed field, the set of positive elements coincides with the set of nonzero squares. This means the
ordering is completely determined by the multiplicative structure of the real closed field.

So let us consider $\mathbb{Q}[\sqrt{2}]$. This is the splitting field of $x^2 - 2$. We see its Galois group has order 2
and that the nonidentity automorphism $\sigma$ must switch the two roots of this polynomial. That is,

$$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$$

for all rationals $a$ and $b$.

The automorphism $\sigma$ behaves almost like complex conjugation. We know our field can be ordered via
the ordering inherited from the field of real numbers. We can get a second ordering just by taking the
image of this usual ordering under the automorphism $\sigma$. This is equivalent to taking

$$P = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q} \text{ and } 0 < a - b\sqrt{2}\}.$$

Of course, we should really check the following conditions:

- For all $u \in \mathbb{Q}[\sqrt{2}]$ exactly one of the following alternatives holds: $u \in P$ or $u = 0$ or $-u \in P$;
- $P$ is closed under addition and multiplication.

This piece of routine work should spice up the life of the hardworking graduate student.

It still remains to show that there are no other orderings or, what is the same, that there are no other
suitable sets for $P$. So let us suppose that $P$ has the two properties itemized above.

What can we deduce about $P$?

Well, every nonzero square is in $P$. Indeed, if $u \neq 0$, then either $u \in P$ or $-u \in P$. In either case,

$$v^2 = u \cdot u = (-u)(-u) \in P$$

since $P$ is closed under products.

So every positive integer is in $P$ since 1 is a square and $P$ is closed under addition.

Also $P$ is closed under the formation of multiplicative inverses. Otherwise there would be a $u \in P$
with $\frac{1}{u} \notin P$. Then $-\frac{1}{u} \in P$. So $-1 = u(-\frac{1}{u}) \in P$, which is impossible since 1 $\in P$.

Hence, each positive rational number belongs to $P$ and, of course, no other rationals belong the
$P$. (This argument would apply in any ordered field and it entails that the smallest subfield—always
isomorphic to the rationals—can only be ordered in one way.)

Of course, either $\sqrt{2} \in P$ or $-\sqrt{2} \in P$. Our approach is to consider first the case $\sqrt{2} \in P$ and prove
that $P = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q} \text{ and } a + b\sqrt{2} > 0\}$. In other words, once we have $\sqrt{2} \in P$ then the usual
ordering is forced on us. Once we have this, we can appeal to the automorphism $\sigma$ to complete the
solution.

Claim
Let $\sqrt{2} \in P$ and $r \in \mathbb{Q}$.

$$r + \sqrt{2} \in P \Leftrightarrow r + \sqrt{2} > 0.$$  

Proof of the Claim. First consider the case when $r \geq 0$. Then $r + \sqrt{2} \in P$ since $P$ is closed under
addition and $r + \sqrt{2} > 0$. Both conditions hold in this case, so they are equivalent.
Consider the case when \( r < 0 \). In this case \(-r \in P\). Now just observe

\[
\begin{align*}
r + \sqrt{2} & \in P \iff r + \sqrt{2} \in P \quad \text{and} \quad -r + \sqrt{2} = -2r + (r + \sqrt{2}) \in P \\
\Rightarrow 2 - r^2 &= (r + \sqrt{2})(-r + \sqrt{2}) \in P \\
\iff 2 - r^2 &> 0 \\
\iff 2 > r^2 > 0 \\
\iff \sqrt{2} > -r > 0 \\
\iff r + \sqrt{2} > 0
\end{align*}
\]

It only remains to reverse the \( \Rightarrow \). Suppose \((r + \sqrt{2})(-r + \sqrt{2}) \in P\). Then either both factors belong to \( P \) or else the negations of both factors belong to \( P \). Hardworking grad students check that this standard fact about positive numbers really holds for all suitable \( P \). But were \(-(-r + \sqrt{2}) \in P\), we would get that \( r \in P \) since we have the \( \sqrt{2} \in P \). But \( r < 0 \), so this is impossible. So it must be that both factors belong to \( P \).

We note, if \( \sqrt{2} \in P \) and \( r \) is rational, then the Claim also gives us

\[
\begin{align*}
r - \sqrt{2} & \in P \iff -r + \sqrt{2} \notin P \iff -r + \sqrt{2} < 0 \iff r - \sqrt{2} > 0.
\end{align*}
\]

(Remember, \( \sqrt{2} \) is not rational.)

Now just consider the following equivalences for any rationals \( a \) and \( b \) with \( b \neq 0 \).

\[
a + b\sqrt{2} \in P \iff b\left(\frac{a}{b} + \sqrt{2}\right) \in P
\]

\[
\iff \text{either } b, \frac{a}{b} + \sqrt{2} \in P \text{ or else } -b, -\left(\frac{a}{b} + \sqrt{2}\right) \in P
\]

\[
\iff \text{either } b > 0 \text{ and } \frac{a}{b} + \sqrt{2} > 0 \text{ or else } b < 0 \text{ and } \frac{a}{b} + \sqrt{2} < 0
\]

Of course, if \( b = 0 \), then \( a + b\sqrt{2} \in P \iff a > 0 \).

It follows that \( P \) is completely determined once we know \( \sqrt{2} \in P \). Since we already know that the set of elements of \( \mathbb{Q}[\sqrt{2}] \) which are positive under the order inherited from the reals is a suitable set of positive elements and it contains \( \sqrt{2} \), then set \( P \) must be the set of positive elements in the usual sense.

So we know what happens when \( \sqrt{2} \in P \).

So we know what happens when \( \sqrt{2} \in P \).

Suppose now that \(-\sqrt{2} \in P \). Let \( P' = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q} \text{ and } \sigma(a + b\sqrt{2}) \in P\} \). Then \( P' \) is a suitable set of positive elements, since \( \sigma \) is an automorphism, and, of course, \( \sqrt{2} \in P' \). But this means, by our reasoning above, that \( P' \) is the usual set of positive elements. So we find

\[
P = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q} \text{ and } a - b\sqrt{2} > 0\}.
\]

(If this bit of reasoning looks circular, it helps to recall that \( \sigma \) is an involution. So \( P' = \sigma(P) \) and \( P = \sigma(P') \) are asserting the same thing.)

So the set of usual positives and the image of this set under \( \sigma \) are the only available notions of positive. There are exactly two orderings of \( \mathbb{Q}[\sqrt{2}] \).
Problem 87.
Prove that $\ln u$ and $\sin u$ are transcendental over the field of rational numbers, whenever $u$ is a positive algebraic real number.

Solution
Let us first consider $\ln u$. Clearly $u = e^{\ln u}$ is an algebraic number, so $\{u\}$ is not algebraically independent over $\mathbb{Q}$. By the Lindemann-Weierstrass Theorem we find that $\ln u$ cannot be algebraic over $\mathbb{Q}$. Hence $\ln u$ is transcendental.

Now consider $\sin u$. Suppose, for contradiction, that $\sin u$ is algebraic. Now $\cos u$ is a root of $x^2 - (1 - \sin^2 u)$. So $\mathbb{Q}[\sin u, \cos u]$ is an algebraic extension $\mathbb{Q}[\sin u]$. Since algebraic extensions of algebraic extensions are algebraic, we would have that $\cos u$ is an algebraic number, as well. Therefore, $e^{ui} = \cos u + i \sin u$ is an algebraic number, since the algebraic numbers constitute a field. By the Lindemann-Weierstrass Theorem, $ui$ cannot be an algebraic number. But of course, it is. So we have our contradiction.

Problem 88.
Let $F$, $K$, and $L$ be fields so that $K$ is a finite separable extension of $F$ and $L$ is a finite separable extension $K$. Prove that $L$ is a finite separable extension of $F$.

Solution
Let $A$ be an algebraic closure $L$. All the fields mentioned in this solution will be subfields of $A$.

Let $u \in L$ and let $f(x)$ be the minimal polynomial of $u$ over $K$. So $f(x)$ is separable. Since $K$ is a finite separable extension of $F$ there is $a \in K$ so that $K = F[a]$. Let $E$ be the subfield of $A$ that is a splitting field of the minimal polynomial $m(x)$ of $a$ over $F$. The polynomial $m(x)$ is separable. Notice that $E$ extends $K = F[a]$. Let $h(x)$ be the minimal polynomial of $u$ over $E$. So $h(x) \mid f(x)$. Since $f(x)$ is separable, so must $h(x)$ be separable. Now $E$ is a Galois extension of $F$ since it is the splitting field of the separable polynomial $m(x)$. Let $G$ be the Galois group of $E$ over $F$. Apply each automorphism in $G$ to the polynomial $h(x)$. Since $G$ is finite, this gives us finitely many images of $h(x)$. Let $h(x) = h_0(x), h_1(x), \ldots, h_{m-1}(x)$ be a listing of all the distinct such images. Let $g(x) = h_0(x)h_1(x) \cdots h_{m-1}(x)$. Now observe that for any $\sigma \in G$ we have that $\sigma(g(x)) = g(x)$ since $\sigma$ permutes the factors of $g(x)$ displayed above. Hence, $g(x) \in F[x]$ since $F$ is the fixed field of $G$. It is evident that $u$, being a root of $h(x)$ is also a root of $g(x)$. We only need to see that $g(x)$ is separable. This follows easily from the following observations:

- Each $h_i(x)$ is irreducible in $E[x]$ since each is the image of the irreducible $h(x)$ under an appropriate automorphism.
- $h_i(x)$ and $h_j(x)$ are relatively prime, if $i \neq j$.
- $h_i(x)$ and $h'_i(x)$ are relatively prime.

Using these facts and some freshman calculus we find that $g(x)$ and $g'(x)$ are relatively prime. So $g(x)$ is separable. This means that $u$, being a root of $g(x)$ is separable over $F$. Hence, $L$ is a separable extension of $F$.

Here is a second route. If the characteristic is $0$, there is really nothing to prove since fields of characteristic $0$ are perfect (every irreducible polynomial is separable). So let us suppose the characteristic is $p \neq 0$. 
First, let \( a, b \in L \) be separable over \( F \) with minimal polynomials \( f(x), g(x) \in F[x] \). These are separable polynomials. Either \( f(x) = g(x) \) or \( f(x)g(x) \) is a separable. Let \( E \) be the splitting field over \( F \) of \( f(x) \) or \( f(x)g(x) \), as the case may be. We have \( a, b \in E \). Then \( E \) is a normal separable extension of \( F \). Hence \( a + b, a \cdot b, a^{-1} \) (if \( a \neq 0 \)) are also separable over \( F \). This means that the set elements of \( L \) separable over \( F \) constitute a subfield \( M \) of \( L \). Evidently, \( M \) extends \( K \).

We aim to show that \( M = L \) to finish the problem. So let \( u \in L \).

Our first step is to show that \( u^{p^n} \) is separable over \( F \) for some \( n \). Let \( m(x) \) be the minimal polynomial of \( u \) over \( F \). If \( m(x) \) is a separable polynomial we are finished. If not there is \( m_1(x) \in F[x] \) with \( m(x) = m_1(x^p) \). So the degree of \( m_1(x) \) is strictly less than the degree of \( m(x) \). If \( m_1(x) \) is separable, then we would have accomplished this step, since \( u^p \) is a root of \( m_1(x) \). Otherwise, we get \( m_2(x) \) with \( m_1(x) = m_2(x^p) \). The degree of \( m_2(x) \) is less than the degree of \( m_1(x) \) and \( u^{p^2} \) is a root of \( m_2(x) \). We can continue in this way only so long, since the degree of \( m(x) \) was finite to begin with. So there will be an \( n \) so that \( u^{p^n} \) is the root of a polynomial in \( F[x] \) that is separable.

Pick \( n \) so that \( u^{p^n} \) is separable over \( F \). So we have \( u^{p^n} \in M \). This means that \( u \) is a root of \( (x - u)^{p^n} \in M[x] \). But \( u \) is separable over \( K \leq M \). This means that the minimal polynomial \( h(x) \) of \( u \) over \( M \) is separable. But \( h(x) \mid (x - u)^{p^n} \). This means that \( h(x) = x - u \). Hence \( u \in M \). Since \( u \) was an arbitrary element of \( L \), we see that \( M = L \). Therefore \( L \) is a separable extension of \( F \).

---

**Problem 89.**

Prove that no finite field is algebraically closed.

---

**Solution**

Fix a prime \( p \) as the characteristic. We know that for every \( q = p^n \), with \( n > 0 \), there is, up to isomorphism, exactly one field of order \( q \). It is the splitting field of \( x^q - x \) over the prime field \( \mathbb{Z}_p \). In particular, the polynomial \( x^q - x \) has \( q \) distinct roots. This means that the algebraic closure of \( \mathbb{Z}_p \) must have at least \( q \) distinct elements. As this must hold for all choices of \( n \) among the positive integers, we see that the algebraic closure of \( \mathbb{Z}_p \) must be infinite. Hence, no finite extension of \( \mathbb{Z}_p \) can be algebraically closed.

Since this is true for every prime \( p \) and since \( \mathbb{Z}_p \) is (isomorphic to) a subfield of every field of characteristic \( p \), we see that no finite field can be algebraically closed.

Here is another proof. It is very brief, but might not be the first thing one thinks about to solve this problem. Let \( F \) be a finite field. Define the map \( \Phi : F \to F \) by \( \Phi(u) = u^2 - u \). Since \( \Phi(0) = 0 = \Phi(1) \) we see that \( \Phi \) is not one-to-one, and, since \( F \) is finite, it follows that \( \Phi \) cannot be onto. Let \( a \) be an element of \( F \) that is not in the image of \( F \) under \( \Phi \). Then \( x^2 - x - a \) cannot have a root in \( F \). Hence \( F \) cannot be algebraically closed.
Problem 90.
Archimedes studied cylinders circumscribed around spheres. Let us say that such a cylinder is constructible provided the radius of the sphere is a constructible real number. So the cylinder circumscribed around a sphere of radius 1 is constructible. Call this cylinder the unit cylinder. Let \( C \) be a cylinder circumscribed around a sphere so that the volume of \( C \) is twice as larger as the volume of the unit cylinder. Explain in detail why \( C \) is not constructible.

**Solution**
The unit cylinder has height 2 and radius 1. So its volume is \( 2\pi \). We would like to have a similar cylinder of volume \( 4\pi \). Say it is circumscribed by a sphere of radius \( r \). So the cylinder would have height \( 2r \) and radius \( r \). So we find \( 4\pi = 2\pi r^3 \). This means that \( 2 = r^3 \). So \( r \) is a root of \( x^3 - 2 \). This polynomial is irreducible by Eisenstein. So Kronecker tells us that \( [\mathbb{Q}[r] : \mathbb{Q}] = 3 \). Since 3 is not a power of 2, we see that \( r \) is not constructible.

---

Problem 91.
Let \( F \) be the subfield of the field of real numbers consisting of all real numbers that are algebraic over the rationals. Prove that there is no irreducible polynomial in \( F[x] \) which has degree 4.

**Solution**
The field \( F \) is a subfield of the field \( \mathbb{R} \) of real numbers. It inherits its ordering (and its set of positive elements) from \( \mathbb{R} \). To see that it is real-closed we need to verify that every polynomial in \( F[x] \) of odd degree has a root in \( F \) and that every positive element of \( F \) has a square root in \( F \). These should be clear since such polynomials (or positive elements) can be regarded over \( \mathbb{R} \). The roots (or square roots) that belong to \( \mathbb{R} \) also belong to \( F \) since they will be algebraic over the rationals. So \( F \) is a real closed field. But then we know that \( F[\sqrt{-1}] \) is the algebraic closure of \( F \) and it is of dimension 2 over \( F \). Let \( f(x) \in F[x] \) be irreducible. Let \( r \in F[\sqrt{-1}] \) be a root of \( f(x) \). The Dimension Formula reveals that \( [F[r] : F] \) must divide 2. Kronecker, on the other hand, tells us that \( [F[r] : F] \) is the degree of \( f(x) \). This means that irreducible polynomials in \( F[x] \) must have degree 1 or degree 2. In particular, they cannot have degree 4.

---

Problem 92.
Let \( R \) be a real closed field and let \( f(x) \in R[x] \). Suppose that \( a < b \) in \( R \) and that \( f(a)f(b) < 0 \). Prove that there is \( c \in R \) with \( a < c < b \) such that \( c \) is a root of \( f(x) \).

**Solution**
This is a version of the Intermediate Value Theorem. We need an algebraic proof so that it will hold in all real closed fields.

It is harmless to suppose that \( f(x) \) is monic (do you see why?). We can factor \( f(x) \) into monic irreducibles over \( R \). Because \( R[\sqrt{-1}] \) is algebraically closed, we can only have irreducibles of degrees 1 and 2. By completing the square, it is easy to verify that if \( x^2 + rx + s \) is irreducible, then \( u^2 + ru + s > 0 \) for all \( u \in R \). This implies that \( f(x) \) must have a linear factor \( g(x) \) such that \( g(a)g(b) < 0 \). Let
\[ g(x) = x - c. \] Then we have \((a - c)(b - c) < 0.\] This means that \(a - c\) and \(b - c\) have opposite signs. It follows that \(a < c < b.\) Evidently, \(c\) is a root of \(f(x).\)

**Problem 93.**
Prove that \(\tan u\) is transcendental over the rationals, for every nonzero algebraic real number \(u.\)

**Solution**
Recall that \(\sec^2 u = 1 + \tan^2 u.\) So \(\tan u\) is algebraic if and only if \(\sec u\) is algebraic. But \(\sec u = \frac{1}{\cos u}.\) So \(\sec u\) is algebraic if and only if \(\cos u\) is algebraic and \(\cos u \neq 0.\) Now \(\cos u = 0\) only at the odd multiples of \(\frac{\pi}{2},\) which we know are not algebraic real numbers. Now check out the solution to Problem 87.

**Problem 94.**
Is \(x^5 - 405x + 5\) solvable by radicals over the field of rational numbers? Prove your answer is correct.

**Solution**
We observe that \(5\) is a prime number and that \(f(x) = x^5 - 405x + 5\) is irreducible by Eisenstein. If we could prove that \(f(x)\) has exactly \(3 = 5-2\) real roots, then we would know that the Galois group of \(f(x)\) over \(\mathbb{Q}\) is \(S_5.\) We know \(S_5\) is not a solvable group, so be Galois \(f(x)\) would not be solvable by radicals.

To see that \(f(x)\) has exactly \(3\) real roots we employ some curve sketching technology from freshman calculus. We see \(f'(x) = 5x^4 - 405 = 5(x^2 + 9)(x - 3)(x + 3).\) This means that \(f(x)\) is strictly increasing on \((-\infty, -3),\) strictly decreasing on \((-3, 3),\) and strictly increasing on \((3, \infty).\) Moreover \(f(-3) = 977\) and \(f(3) = -967,\) which are, respectively, the local maximum and local minimum of \(f(x).\) It follows that \(f(x)\) crosses the X-axis three times (at our desired roots): once when \(x < -3,\) once when \(-3 < x < 3,\) and once when \(3 < x.\)