Math 351

Solutions to review problems for Final Exam December 11, 2010

#1 (a) Find the greatest common divisor of 182 and 507 and write it in the form $a(182) + b(507)$ where $a$ and $b$ are integers.

Solution:

$$507 - 2(182) = 143,$$
$$182 - 143 = 39,$$
$$143 - 3(39) = 26,$$
$$39 - 26 = 13,$$
$$26 - 2(13) = 0.$$

Therefore $(182, 507) = 13$ since this is the last nonzero remainder. Furthermore,


(b) Find the greatest common divisor of $x^4 + x^2 - 20$ and $x^4 - 4x^3 + 5x^2 - 4x + 4$ in $\mathbb{Q}[x]$.

Solution:

$$(x^4 - 4x^3 + 5x^2 - 4x + 4) - (x^4 + x^2 - 20) = (-4x^3 + 4x^2 - 4x + 24),$$
$$(x^4 + x^2 - 20) - (-x/4 - 1/4)(-4x^3 + 4x^2 - 4x + 24) = (x^2 + 5x - 14),$$
$$(-4x^3 + 4x^2 - 4x + 24) - (-4x + 24)(x^2 + 5x - 14) = (-180x + 360),$$
$$(x^2 + 5x - 14) - (-x/180 - 7/180)(-180x + 360) = 0.$$

Therefore $(x^4 - 4x^3 + 5x^2 - 4x + 4, x^4 + x^2 - 20) = x - 2$. This is the monic polynomial which is an associate of the last nonzero remainder.

(c) Find the greatest common divisor of $x^5 + x^4 + x^3 + 1$ and $x^5 + x + 1$ in $\mathbb{Z}_2[x]$ and write it in the form $a(x)(x^5 + x^4 + x^3 + 1) + b(x)(x^5 + x + 1)$ where $a(x), b(x) \in \mathbb{Z}_2[x]$.

Solution:

$$(x^5 + x^4 + x^3 + 1) + (x^5 + x + 1) = (x^4 + x^3 + x),$$
$$(x^5 + x + 1) + (x + 1)(x^4 + x^3 + x) = (x^3 + x^2 + 1),$$
$$(x^4 + x^3 + x) + x(x^3 + x^2 + 1) = 0.$$

Therefore $(x^5 + x^4 + x^3 + 1, x^5 + x + 1) = x^3 + x^2 + 1$ since this is the last nonzero remainder. Furthermore,

$$(x^3 + x^2 + 1) = (x^5 + x + 1) + (x + 1)(x^4 + x^3 + x) =$$
\[ (x^5 + x + 1) + (x + 1)((x^5 + x^4 + x^3 + 1) + (x^5 + x + 1)) = \]
\[ x(x^5 + x + 1) + (x + 1)(x^5 + x^4 + x^3 + 1). \]

\#2 (a) Let \( R \) be a commutative ring with unit and \( a \in R \). Recall that \( (a) \) denotes \( \{ar \mid r \in R \} \). Prove that \( (a) \) is an ideal in \( R \).

**Solution:** \( 0 = a0 \in (a) \), so \( (a) \neq \emptyset \). Let \( x_1, x_2 \in (a), r \in R \). Then \( x_1 = as_1, x_2 = as_2 \) for some \( s_1, s_2 \in R \). Then \( x_1 + x_2 = as_1 - as_2 = a(s_1 - s_2) \in (a) \), \( x_1r = (ax_1)r = a(s_1r) \in (a) \), and \( rx_1 = x_1r \in (a) \). Thus \( (a) \) is an ideal.

(b) Let \( F \) be a field and \( I \) be an ideal in \( F[x] \). Prove that \( I = (f(x)) \) for some \( f(x) \in F[x] \).

**Solution:** If \( I = \{0\} \), then \( I = (0) \) and the result holds. If \( I \neq \{0\} \), then \( I \) contains a nonzero element and so the set \( J = \{\text{deg}(g(x)) \mid g(x) \in I, g(x) \neq 0\} \) is a nonempty set of nonnegative integers. Therefore \( J \) contains a smallest element, say \( m \). Let \( f(x) \in I \) be of degree \( m \). Then, \( (f(x)) \subseteq I \). Let \( g(x) \in I \). Then, by the division algorithm,

\[ g(x) = f(x)q(x) + r(x) \]

for some polynomials \( q(x) \) and \( r(x) \) with \( r(x) = 0 \) or \( \text{deg}(r(x)) < \text{deg}(f(x)) = m \). Now

\[ r(x) = g(x) - f(x)q(x) \in I. \]

If \( r(x) \neq 0 \), then \( \text{deg}(r(x)) \in J \), contradicting the fact that \( m \) is the smallest element of \( J \). Thus \( r(x) = 0 \) so \( g(x) = f(x)q(x) \in (f(x)) \). Thus \( I \subseteq (f(x)) \) and so \( I = (f(x)) \).

(c) Give an example of a commutative ring with unit \( R \) and an ideal \( I \) in \( R \) which is not equal to \( (a) \) for any \( a \in R \).

**Solution:** Let \( R = \mathbb{Z}[x] \) and let \( I \) be the set of all polynomials in \( \mathbb{Z}[x] \) with even constant term. Then \( I \) is an ideal, \( 2 \in I \) and \( x \in I \). If \( I = (a) \), then \( a \) divides \( 2 \) so \( a \) is a constant polynomial. Since \( (a) = (|a|) \) we may assume that \( a = 1 \) or \( 2 \). But \( 1 \notin I \) (since \( 1 \) is not even), so \( a = 2 \). But \( x \in I \) and \( 2 \) does not divide \( x \). This contradiction shows that \( I = (a) \) is impossible.

\#3 Let \( R \) be a ring and \( S \) be a subring in \( R \). Suppose that whenever \( a, a_1, b, b_1 \in R \) satisfy \( a - a_1 \in S \) and \( b - b_1 \in S \) we have \( ab - a_1b_1 \in S \). Prove that \( S \) is an ideal in \( R \).

**Solution:** Since \( S \) is a subring, we only need to show that if \( s \in S \) and \( r \in R \), then \( rs \in S \) and \( sr \in S \). First let \( a = a_1 = r, b = s, b_1 = 0 \). Then \( a - a_1 = 0 \in S \) and \( b - b_1 = s = s \in S \). Hence \( ab - a_1b_1 = rs - 0 = rs \in S \). Next let \( a = s, a_1 = 0 \) and \( b = b_1 = r \). Then \( a - a_1 = s - 0 \in S \) and \( b - b_1 = r - r = 0 \in S \). Hence \( ab - a_1b_1 = sr - 0r = sr \in S \).

\#4 (a) Let \( F \) be a field. Prove that the only units in \( F[x] \) are the nonzero constant polynomials.

**Solution:** If \( f(x) \) is a unit, then \( f(x)g(x) = 1 \) for some \( g(x) \). Then both \( f(x) \) and \( g(x) \) must be nonzero. Furthermore, we have \( \text{deg}(f(x)g(x)) = \text{deg}(f(x)) + \text{deg}(g(x)) \)
for any nonzero \( f(x), g(x) \in F[x] \). Since \( \text{deg}(1) = 0 \) this shows that if \( f(x)g(x) = 1 \)
then \( \text{deg}(f(x)) = \text{deg}(g(x)) = 0 \). This means that \( f(x) \) and \( g(x) \) are nonzero constant
polynomials.

(b) What are the units in \( \mathbb{Z}[x] \)? Why?

**Solution:** The argument in the previous part shows that any unit must be a constant
polynomial, hence a nonzero integer. The only integers that are units (in \( \mathbb{Z} \)) are 1 and -1.

(c) What are the units in \( \mathbb{Z} \times \mathbb{Z} \)? Why?

**Solution:** The identity element in \( \mathbb{Z} \times \mathbb{Z} \) is \((1,1)\). Thus if \((a,b)\) is a unit in \( \mathbb{Z} \times \mathbb{Z} \) we must
have \((ac,bd) = (a,b)(c,d) = (1,1)\) for some \(c,d \in \mathbb{Z}\). Thus \(a\) and \(b\) are units in \( \mathbb{Z} \). Using
the result of the previous part, we see that the units in \( \mathbb{Z} \times \mathbb{Z} \) are \((1,1),(1,-1),(-1,1)\)
and \((-1,-1)\).

#5 Let \( R \) be a ring and \( I \) be an ideal in \( R \). Let \( J \) be a subring of \( R/I \). Prove that there
is some subring \( K \) of \( R \) such that \( K \supseteq I \) and \( J = K/I \). Then show that \( J \) is an ideal in
\( R/I \) if and only if \( K \) is an ideal in \( R \). Finally, show that if \( J \) is an ideal then \( (R/I)/J \) is
isomorphic to \( R/K \).

**Solution:** Let \( K = \{ r \in R | r + I \in J \} \). Then \( 0 \in K \), so \( K \neq \emptyset \). If \( r_1, r_2 \in K \), then
\( r_1 + I, r_2 + I \in J \) and so \((r_1 - r_2) + I = (r_1 + I) - (r_2 + I) \in J \) so \( r_1 - r_2 \in K \). Also
\( r_1 r_2 + I = (r_1 + I)(r_2 + I) \in J \) so \( r_1 r_2 \in K \). Thus \( K \) is a subring of \( R \).

Now suppose \( J \) is an ideal in \( R/I \), \( r \in K \), and \( s \in R \). Then \( sr + I = (s + I)(r + I) \in J \)
and \( rs + I = (r + I)(s + I) \in J \). Hence \( sr \in K \) and \( rs \in K \). Thus \( K \) is an ideal in \( R \). On
the other hand, if \( K \) is an ideal in \( R \) and \( x \in J, y \in R/I \), then \( x = r + I \) for some \( r \in K \)
and \( y = s + I \) for some \( s \in R \). Then \( xy = (r + I)(s + I) = rs + I \). Since \( K \) is an ideal in
\( R \), \( rs \in K \) and so \( xy \in J \). Similarly, \( yx = (s + I)(r + I) = sr + I \). Since \( K \) is an ideal in
\( R \), \( sr \in K \) and so \( yx \in J \). Thus \( J \) is an ideal in \( R/I \).

Now define a map \( \phi : R/I \to R/K \) by \( \phi(r + I) = r + K \). It is easy to see that this
is a surjective homomorphism with kernel \( J \). Then the first isomorphism theorem shows
that \( (R/I)/J \) is isomorphic to \( R/K \).

#6 Let \( M(\mathbb{Z}) \) denote the ring of 2 by 2 matrices over \( \mathbb{Z} \).

(a) Let \( W \) denote \( \{ \begin{vmatrix} a & b \\ 0 & c \end{vmatrix} \mid a, b, c \in \mathbb{Z} \} \subseteq M(\mathbb{Z}) \), Show that \( W \) is a subring of \( M(\mathbb{Z}) \).

**Solution:** The zero matrix is in \( W \), so \( W \) is nonempty. Let
\( \begin{vmatrix} a & b \\ 0 & c \end{vmatrix}, \begin{vmatrix} a_1 & b_1 \\ 0 & c_1 \end{vmatrix} \in W \). Then
\( \begin{vmatrix} a & b \\ 0 & c \end{vmatrix} - \begin{vmatrix} a_1 & b_1 \\ 0 & c_1 \end{vmatrix} = \begin{vmatrix} a - a_1 & b - b_1 \\ 0 & c - c_1 \end{vmatrix} \in W \)
and
\( \begin{vmatrix} a & b \\ 0 & c \end{vmatrix} \begin{vmatrix} a_1 & b_1 \\ 0 & c_1 \end{vmatrix} = \begin{vmatrix} aa_1 & ab_1 + bc_1 \\ 0 & cc_1 \end{vmatrix} \in W \).

Thus \( W \) is a subring.
(b) Let $S$ denote the set of all symmetric matrices in $M(\mathbb{Z})$. Is $S$ a subring? Why or why not?

**Solution:** $\begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix}$ and $\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$ are symmetric matrices, but their product $\begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}$ is not symmetric.

(c) Let $G$ denote the group of units of $W$. What is $G$?

**Solution:** Since $\begin{vmatrix} ab \\ 0 \\ c \end{vmatrix}$ $\begin{vmatrix} a \\ 1 \\ b \\ 0 \\ c \\ 1 \end{vmatrix} = \begin{vmatrix} aa \\ 0 \\ ab \\ 1 \end{vmatrix} = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$ the matrix $\begin{vmatrix} a \\ b \\ 0 \\ c \end{vmatrix}$ can be a unit only if $a$ and $c$ are units in $\mathbb{Z}$, that is, only if $a$ is 1 or $-1$ and $c$ is 1 or $-1$. This implies that $a^2 = c^2 = 1$. Then, for such $a$ and $c$ and for any $b \in \mathbb{Z}$,

$\begin{vmatrix} a \\ b \\ 0 \\ c \end{vmatrix} \begin{vmatrix} a \\ -abc \\ 0 \\ c \end{vmatrix} = \begin{vmatrix} a^2 \\ 0 \\ -a^2bc + bc \end{vmatrix} = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$.

Thus, if $a = \pm 1$, $c = \pm 1$, $b \in \mathbb{Z}$, $\begin{vmatrix} a \\ b \\ 0 \\ c \end{vmatrix}$ is a unit and

$\begin{vmatrix} a \\ b \\ 0 \\ c \end{vmatrix}^{-1} = \begin{vmatrix} a \\ -abc \\ 0 \\ c \end{vmatrix}$.

Therefore

$G = \{ \begin{vmatrix} a \\ b \\ 0 \\ c \end{vmatrix} | a = \pm 1, c = \pm 1, b \in \mathbb{Z} \}$.

(d) Let $N = \{ \begin{vmatrix} 1 \\ b \\ 0 \\ 1 \end{vmatrix} | b \in \mathbb{Z} \}$. Show that $N$ is a normal subgroup of $G$.

**Solution:** First of all, $N$ is a subgroup of $G$ since

$\begin{vmatrix} 1 \\ b \\ 0 \\ 1 \end{vmatrix} \begin{vmatrix} 1 \\ b' \\ 0 \\ 1 \end{vmatrix} = \begin{vmatrix} 1 \\ b + b' \end{vmatrix} \in N$

and so $\begin{vmatrix} 1 \\ b \\ 0 \\ 1 \end{vmatrix}^{-1} = \begin{vmatrix} 1 \\ -b \\ 0 \\ 1 \end{vmatrix} \in N$. Let $g \in G$ and $n = \begin{vmatrix} 1 \\ b \\ 0 \\ 1 \end{vmatrix} \in N$. Then, by the previous part, $g = \begin{vmatrix} a \\ d \\ 0 \\ c \end{vmatrix}$ where $a^2 = c^2 = 1$ and $d \in \mathbb{Z}$ and

$gng^{-1} = \begin{vmatrix} a \\ d \\ 0 \\ c \end{vmatrix} \begin{vmatrix} 1 \\ b \\ 0 \\ 1 \end{vmatrix} \begin{vmatrix} a \\ -acd \\ 0 \\ c \end{vmatrix} = \begin{vmatrix} a \\ ab + d \\ 0 \\ c \end{vmatrix} \begin{vmatrix} a \\ -adc \\ 0 \\ c \end{vmatrix} = \begin{vmatrix} a^2 \\ -a^2dc + abc + cd \end{vmatrix} = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$.
Thus \( N \) is a normal subgroup of \( G \)

(e) Describe \( G/N \).

Solution: There are four cosets of \( N \) in \( G \):

\[
N = N \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},
\]

\[
N \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},
\]

\[
N \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},
\]

and

\[
N \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.
\]

Hence \( G/N \) is isomorphic to the group of units of \( \mathbb{Z} \times \mathbb{Z} \).

#7 (a) Find all monic irreducible polynomials of degree 3 over \( \mathbb{Z}_3 \).

Solution: A polynomial of degree 3 over a field is irreducible if and only if it has no roots. The monic polynomial \( x^3 + ax^2 + bx + c \) has root 0 if and only if \( c = 0 \), has root 1 if and only if \( 1 + a + b + c = 0 \), and has root 2 if and only if \( 2 + a + 2b + c = 0 \). When these possibilities are eliminated, the following 8 irreducible monic polynomials of degree 3 remain:

\[
x^3 + 2x^2 + x + 1, x^3 + 2x + 1, x^3 + x^2 + 2x + 1, x^3 + 2x + 1,
\]

\[
x^3 + 2x^2 + 2x + 2, x^3 + x^2 + x + 2, x^3 + x^2 + 2, x^3 + 2x + 2.
\]

(b) Find all irreducible polynomials of degree 4 over \( \mathbb{Z}_2 \).

Solution: A polynomial of degree 4 is reducible if and only if it has a root or an irreducible factor of degree 2. Since the only irreducible polynomial of degree 2 over \( \mathbb{Z}_2 \) is \( x^2 + x + 1 \), a polynomial of degree 4 is reducible if and only if it has a root or is \( (x^2 + x + 1)^2 = x^4 + x^2 + 1 \). Now the polynomial \( x^4 + ax^3 + bx^2 + cx + d \) has a root if and only if either \( d = 0 \) or \( a + b + c + d = 1 \). When these possibilities are eliminated, the following 3 irreducible monic polynomials of degree 4 remain:

\[
x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1.
\]

#8 (a) Let \( I \) be a nonzero ideal in \( \mathbb{Z} \). Prove that \( \mathbb{Z}/I \) is a field if and only if it is an integral domain.

Solution: Since \( I \) is nonzero, \( I = (a) \) for some positive integer \( a \). Then \( \mathbb{Z}/I \) is an integral domain if and only if \( a \) is prime and is a field if and only if \( a \) is prime.
(b) Let $F$ be a field and $J$ be a nonzero ideal in $F[x]$. Prove that $F[x]/J$ is a field if and only if it is an integral domain.

**Solution:** Since $J$ is nonzero, $J = (f(x))$ for some nonzero polynomial $f(x)$. Then $F[x]/J$ is an integral domain if and only if $f(x)$ is irreducible and is a field if and only if $f(x)$ is irreducible.

(c) Let $R$ be a finite ring and $L$ be an ideal in $R$. Prove that $R/L$ is a field if and only if it is an integral domain.

**Solution:** Any field is an integral domain and any finite integral domain is a field.

(d) Give an example of a ring $R$ and a nonzero ideal $K$ in $R$ such that $R/K$ is an integral domain but not a field.

**Solution:** For example, $R = \mathbb{Z} \times \mathbb{Z}$ and $K = \{(0,n) | n \in \mathbb{Z}\}$.

#9 Let $G$ be a group with identity $e$. Prove that:

(a) If $x^2 = e$ for all $x \in G$, then $G$ is abelian.

**Solution:** Let $x, y \in G$. Then $xyxy = (xy)^2 = e$ and so $x(xyxy)y = xey = xy$. But $x(xyxy)y = x^2yxy^2 = eyxe = yx$.

(b) If $G$ is abelian and finite and $h$ is the product of all of the elements of $G$, then $h^2 = e$.

**Solution:** Suppose $G = \{g_1, ..., g_n\}$. Then $h = g_1g_2...g_n$. Now we also have $G = \{g_1^{-1}, ..., g_n^{-1}\}$ (since the map that takes each element to its inverse is a bijection). Thus $h = g_1^{-1}...g_n^{-1}$. Then $h^2 = (g_1...g_n)(g_1^{-1}...g_n^{-1})$. Since $G$ is abelian, this product is $e$.

#10 Let $G$ be a cyclic group of order 374? How many subgroups does $G$ have?

**Solution:** There is one subgroup for every divisor of 374. Since $374 = 2 \times 11 \times 17$ it has 8 divisors.

#11 Find all the (right) cosets of $(2\mathbb{Z}) \times (3\mathbb{Z})$ in $\mathbb{Z} \times \mathbb{Z}$.

**Solution:** Any coset can be represented by a pair $(a, b)$ where $0 \leq a < 2, 0 \leq b < 3$ and no two of these pairs are in the same coset. Thus, letting $M = (2\mathbb{Z}) \times (3\mathbb{Z})$ the cosets of $M$ in $\mathbb{Z} \times \mathbb{Z}$ are:

$$M = M + (0, 0), M + (0, 1), M + (0, 2), M + (1, 0), M + (1, 1), M + (1, 2).$$

#12 Suppose that $G$ is a group and $H, K$ are normal subgroups of $G$ with $H \cap K = \{e\}$. Prove that $hk = kh$ for any $h \in H, k \in K$.

**Solution:** Let $h \in H, k \in K$. Consider the element $u = (hk)(kh)^{-1} = hkh^{-1}k^{-1}$. Since $K$ is normal, we have that $hkh^{-1} \in K$ and so

$$u = (hkh^{-1})k \in K.$$
Also, since $H$ is normal, we have that $kh^{-1}k^{-1} \in H$ and so
\[ u = h(kh^{-1}) \in H. \]
Thus $u \in H \cap K = \{e\}$ so $u = (hk)(kh)^{-1} = e$. Thus $hk = kh$.

#13 Let $C(n)$ denote the cyclic group of order $n$.
(a) Find all abelian groups of order 792 and write each in the form
\[ C(n_1) \oplus \ldots \oplus C(n_k) \]
where $n_i$ divides $n_{i+1}$ for each $i, 1 \leq i \leq k - 1$.

Solution: It is easiest to do part (b) first and then rewrite each of the expressions there by using the fact that if $(m,n) = 1$ then $C(m) \oplus C(n)$ is isomorphic to $C(mn)$. This gives:
\[ C(792), \]
\[ C(3) \oplus C(264), \]
\[ C(2) \oplus C(396), \]
\[ C(6) \oplus C(132), \]
\[ C(2) \oplus C(2) \oplus C(198), \]
\[ C(2) \oplus C(6) \oplus C(66). \]

(b) Find all abelian groups of order 792 and write each in the form
\[ C(p_1^{m_1}) \oplus \ldots \oplus C(p_l^{m_l}) \]
where $p_1, \ldots, p_l$ are distinct primes and $m_1, \ldots, m_l$ are positive integers.

Solution: Since $792 = 2^3 \times 3^2 \times 11$ we see that the (six) possibilities for the group are
\[ C(2^3) \oplus C(3^2) \oplus C(11), \]
\[ C(2^3) \oplus C(3) \oplus C(3) \oplus C(11), \]
\[ C(2) \oplus C(2^2) \oplus C(3^2) \oplus C(11), \]
\[ C(2) \oplus C(2^2) \oplus C(3) \oplus C(3) \oplus C(11), \]
\[ C(2) \oplus C(2) \oplus C(2) \oplus C(3^2) \oplus C(11), \]
\[ C(2) \oplus C(2) \oplus C(2) \oplus C(3) \oplus C(3) \oplus C(11). \]

(c) How many abelian groups of order 7! are there (up to isomorphism)? Since $7! = 2^4 \times 3^2 \times 5 \times 7$ the number of abelian groups of order 7! is the product of the number of abelian groups of order $2^4$ (which is 5), the number of abelian groups of order $3^2$ (which is
2), the number of abelian groups of order 5 (which is 1), and the number of abelian groups of order 7 (which is 1). Thus the number of abelian groups of order 7! is 10.

# 14 Show that there is no simple group of order 483.

**Solution:** Let $G$ be a group of order 483. Since $483 = 3 \times 7 \times 23$, the third Sylow Theorem shows that the number of Sylow 23-subgroups is of the form $1 + k(23)$ and that this number divides $3 \times 7 \times 23$. Since $(1 + k(23), 23) = 1$ we must have that $1 + k(23)$ divides $3 \times 7 = 21$. Then $1 + k(23)$ must be less than or equal to 21. This means $k = 0$ and so the number of Sylow 23-subgroups is 1. But if $H$ is a Sylow 23-subgroup, so is $gHg^{-1}$ for any $g \in G$. Hence $H = gHg^{-1}$ for any $g \in G$. Thus $H$ is a normal subgroup of $G$ and so $G$ is not simple.

#15 (a) Let $\sigma \in S_9$ be

$$(148)(26)(3759).$$

Express $\sigma$ as a product of disjoint cycles.

**Solution:** $(148)(26)(3759)$

(b) Write $\sigma$ in table form.

**Solution:**

\[
\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
4 & 6 & 7 & 8 & 9 & 2 & 5 & 1 & 3
\end{bmatrix}
\]

(c) Suppose $\sigma$ (from the previous part) is written as a product of $k$ transpositions. Is $k$ even or odd? Why?

**Solution:** Any $k$-cycle can be written as a product of $k - 1$ transpositions. The original expression for $\sigma$ is a product of two 4-cycles and a 5-cycle. Thus this can be written as a product of 10 transpositions. Thus if $\sigma$ can be written as a product of $k$ transpositions, $k$ must be even.