Group Theory

Jan 2012 #6
Prove that if $G$ is a nonabelian group, then $G/Z(G)$ is not cyclic.
Sol: Suppose on the contrary, $G/Z(G)$ is generated by $aZ(G)$.
Every element $g = a^kh$, $k \in \mathbb{Z}$, $h \in Z(G)$.
\[ a^kh \times a^rs = a^{k+r}hs = a^r s \times a^kh \rightarrow \]

Aug 2011 #9 (Jan 2010 #5)
Prove that any group of order $p^2$ is an abelian group.
Sol: $P$-groups has non-trivial center due to class formula, then follow from the above question.

Jan 2012 #7
$G$ is nonabelian finite group of order $p^3$, prove $Z(G) = [G, G]$.
Sol: Again, $P$-groups has non-trivial center. $G$ is non abelian implies $\{ e \} \subset Z(G) \subset G$ and $|G, G| \neq \{ e \}$.
$G/Z(G)$ has order $p$ or $p^2$. From Jan 2012 #6, $G/Z(G)$ is not cyclic, so $G/Z(G)$ is an abelian group(by Aug 2011 #9) of order $p^2$.
But then $Z(G) \supset [G, G]$. From the order, they are equal.

Aug 2011 #12
$G$ is a finite group, and $M \subset G$ be a maximal subgroup.
Show that if $M$ is normal subgroup of $G$, then $|G : M|$ is prime.
Sol: $G/M$ is a group with no non-trivial proper subgroup. So it is generated by any $gM$ with $g \notin M$.
So $G/M$ is cyclic and the order must be prime.

Jan 2011 #1 (Aug 2010 #8)
Find the element $g$ of order 2 in $S_6$ with minimal order of the centralizer $C(g) = \{ h \in G \mid hg = gh \}$.
Find the numbers of element in $S_6$ that commute with $g \in S_5$ where $g$ has order 6.
Sol: $g$ must conjugate to either $(1,2), (1,2)(3,4)$ or $(1,2)(3,4)(5,6)$.
The orbit of $(1,2)$ under conjugation is of size $C(6,2) = 15$
The orbit of $(1,2)(3,4)$ under conjugation is of size $C(6,2)C(4,2)/2 = 45$
The orbit of $(1,2)(3,4)(5,6)$ under conjugation is of size $5 \times 3$
So the centralizer are of size $6! /15.6! \div 45.6! /15$.
Hence $(1,2)(3,4)$ has minimal order 16.
A direct computation can find centralizer.
\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
2 & 1 & 3 & 4 & 5 & 6
\end{pmatrix}
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
a & b & c & d & e & f
\end{pmatrix}
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
2 & 1 & 3 & 4 & 5 & 6
\end{pmatrix}
= \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
a & b & c & d & e & f
\end{pmatrix}
\]
Hence a,b is either 1,2 and c,d,e,f can be any number 3-6,etc

Aug 2010 #2
Let $G$ be a finite group and $\Phi : G \rightarrow G$ be an automorphism.
1. Show that $\Phi$ maps a conjugacy class of $G$ into a conjugacy class of $G$.
2. Give an example of non-trivial $G$ and $\Phi$ such that $\{ e \}$ is the only conjugacy class of $G$ that maps into itself.
   Explain.
3. Show that if $G = S_5$, then $g$ and $\Phi(g)$ must be conjugate for any $g \in G$.
Sol: $\Phi(a^{-1}ga) = \Phi(a)^{-1}\Phi(g)\Phi(a)$.
$G := C_2 \times C_2$, $\Phi((x, y)) = (y, x + y)$ and $G$ is abelian.
The conjugacy class is of size $1^{e^2}, 10^{(1,2)^5}, 15^{(1,2)(3,4)^5}, 20^{(1,2,3)^5}, 30^{(1,2,3,4)^5}, 24^{(1,2,3,4,5)^5}, 20^{(1,2,3)(4,5)^5}$
By part 1 and the order of the element.

Jan 2010 #6
How many conjugacy classes are there in the symmetric group $S_5$.
Sol: 7 from above.
Jan 2010 #4
Suppose $G$ is a group of order 60 that has 5 conjugacy classes of orders 1, 15, 20, 12, 12.
Prove that $G$ is a simple group.
Sol: A normal subgroup $N$ is a subgroup of $G$ and is disjoint union of conjugacy class in $G$.
The numbers above can’t form a subgroup.

Aug 2010 #5
Let $G$ be the group of rigid motions (more specifically, rotations) in $\mathbb{R}^3$ generated by $a$ = a 90 degree rotation about $x$–axis, and $b$ = a 90 degree rotation about $y$–axis.

1. How many elements does $G$ have?
2. Show that the subgroup generated by $a^2$ and $b^2$ is a normal subgroup of $G$.

Sol: $a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Show that $G$ is the set of matrix with only one nonzero entry which is 1 in each row and column and the determinant is 1. Hence order of $G = 24$.

$c := bab^{-1} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ = a 90 degree rotation about z-axis. Now it is not hard to see it is the automorphism group of a cube and hence has 24 elements.

$a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$, $b^2 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $a^2b^2 = c^2$ so this group generate four element and is isomorphic to Klein 4 group.

It is sufficient to check $b^{-1}a^3b$ and $a^{-1}b^2a$ is in this subgroup.

$b^{-1}a^3b = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix}$ and $a^{-1}b^2a = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$

Jan 2012 #5
Let $a$, $b$ be elements of a group $G$. Prove that $ab$ and $ba$ have the same order.
Sol: $a(bab...ab) = 1$ implies $bab...ab$ is the inverse of $a$ implies $(bab...ab)a = 1$. (Left inverse = Right inverse)

Jan 2012 #8
Determine the group of $Aut(C_4 \times C_2)$, calculating its order and identifying it with a familiar group.
Sol: Denote $G = C_4 \times C_2 = \{e, a, b, c\}$ where $c = ab$.
The automorphism on $G$ is the permutation on $\{a, b, c\}$. So $Aut(C_4 \times C_2) = S_3$.
Or $Aut(C_4 \times C_2) = GL_2(\mathbb{F}_2)$.

Aug 2011 #11
Find the cardinality of $Hom(\mathbb{Z}/20\mathbb{Z},\mathbb{Z}/50\mathbb{Z})$.
Sol: Suppose $\phi \in Hom(\mathbb{Z}/20\mathbb{Z},\mathbb{Z}/50\mathbb{Z})$. Say $\phi(1) = n$. Then $20n = 0$, hence $5|n$.
So $n$ can be $0, 5, 10, 15, ..., 45$. Hence $Hom(\mathbb{Z}/20\mathbb{Z},\mathbb{Z}/50\mathbb{Z}) \cong \mathbb{Z}/10\mathbb{Z}$.

Jan 2011 #3
Show that every finite group of order $\geq 3$ has a non-trivial automorphism.
Sol: If $G$ is abelian, then $G$ is a product of cyclic group. And each such group has non-trivial automorphism.
(at least $\mathbb{Z}/n\mathbb{Z}$, $n > 2$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are contain in $G$)
If $G$ is not abelian, then there is $a, b \in G$ such that $ab \neq ba$. Define $\phi_a$ by $\phi_a(g) = a^{-1}ga$.

Jan 2010 #8
1. Show that $Hom(G,H)$ is an abelian group if $H$ is abelian group.
2. Prove that if $G$ is finite cyclic group, then $Hom(G,\mathbb{Q}/\mathbb{Z})$ is isomorphic to $G$. 
3. Find an infinite abelian group $G$ such that $\text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ is not isomorphic to $G$.

Sol: $f_1(gh) + f_2(gh) = f_1(g) + f_1(h) + f_2(g) + f_2(h) = f_1(g) + f_2(g) + f_1(h) + f_2(h)$. So $f_1 + f_2$ is a homomorphism. And it is clear that $f_1 + f_2 = f_2 + f_1$ pointwise.

If $G = \mathbb{Z}/n\mathbb{Z}$, then $f(1) = \alpha \in \mathbb{Q}/\mathbb{Z}$. Then $n\alpha = 0$ implies $\alpha = \frac{k}{n}$, $0 \leq k < n$. Hence $\text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ is finite cyclic and generated by $f(1) = \frac{1}{n}$.

Let $G = \mathbb{Z}$ and $f(1) = \alpha$. Then $\alpha$ can any element in $\mathbb{Q}/\mathbb{Z}$. And hence $\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$. But $\mathbb{Q}/\mathbb{Z}$ is not cyclic.

Aug 2011 #10

Let $a \in G$. Prove that $a$ commutes with each of its conjugates in $G$ iff $a$ belongs to an abelian normal subgroup of $G$.

Sol: ($\Rightarrow$) Define $N = \langle g^{-1}ag \rangle$, $g \in G$.

($\Leftarrow$) Let $N$ be the abelian normal subgroup. Then $g^{-1}ag \in N$ and hence commute with $a$.

Jan 2011 #2

Let $G$ be a group and $H_3$ and $H_5$ be normal subgroups of $G$ of index 3 and 5 respectively.

Prove that every element of $g \in G$ can be written in the form $g = h_3h_5$ with $h_3 \in H_3$ and $h_5 \in H_5$.

Sol: Let $\pi : G \rightarrow G/H_5$. Then $\pi(H_3) \not\subseteq eH_5 \Leftrightarrow H_3 \not\subseteq H_5$. Hence $\pi(H_3)$ is a nontrivial subgroup of $G/H_5 \cong \mathbb{Z}/5\mathbb{Z}$. So $\pi(H_3) = G/H_5$. So for all $g \in G$, there is $h_3 \in H_3$ s.t. $\pi(g) = \pi(h_3)$.

- Linear Algebra part 1

Aug 2011 #2

Let $V$ be a finite dimensional real vector space of dimension $n$. Define an equivalence relation $\sim$ on the set $\text{End}_\mathbb{R}(V)$ of $\mathbb{R}$-linear homomorphisms $V \rightarrow V$ as follows:

if $S, T \in \text{End}_\mathbb{R}(V)$ then $S \sim T$ if there are invertible maps $A, B : V \rightarrow V$ s.t. $S = BTA$.

Determine, as a function of $n$, the number of equivalence classes.

Sol: Any $S$ can be reduced to row echelon form by row operation and hence by an invertible matrix $A$. Then by suitable column operation, then get a matrix in row reduced form and the leading one is at (i,i)-entry for i from 1 to $r$ where $r$ is the rank.

So $f(n) = n + 1$.

Aug 2010 #3

Let $V$ and $W$ be real vector spaces, and let $T : V \rightarrow W$ be a linear map. If the dimensions of $V$ and $W$ are $3$ and $5$, respectively, then for any bases $B$ of $V$ and $B'$ of $W$, we can represent $T$ by a $5 \times 3$ matrix $A_{T,B,B'}$. Find a set $S$ of $5 \times 3$ matrices as small as possible such that for any $T : V \rightarrow W$ there are bases $B$ of $V$ and $B'$ of $W$ such that $A_{T,B,B'} \in S$.

Sol: Similar to last one.

Jan 2011 #5

Let $T : \mathbb{R}^4 \rightarrow \mathbb{R}^2$ be the linear transformation $T(a, b, c, d) = (a + b - c, c + d)$. Find a basis for the null space.

Sol: \[
\begin{bmatrix}
1 & 1 & -1 & 0 \\
0 & 0 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 & -1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0
\end{bmatrix}
\rightarrow
\begin{bmatrix}
1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0
\end{bmatrix}
\]

$(−b − d, b, −d, d) = b(−1, 1, 0, 0) + d(−1, 0, −1, 1)$.

Jan 2010 #7

Let $G = GL_2(\mathbb{F}_5)$. What is the order of $G$?

Sol: $(25−1)(25−5) = 480$.

Jan 2010 #3

Let $A, B$ be $n \times n$ complex matrices such that $AB = BA$. Prove that there exists a vector $v \neq 0$ in $\mathbb{C}^n$ which is an eigenvector for $A$ and for $B$.

Sol: Let $\lambda$ be an eigenvalue of $\Phi_A$ where $\Phi_A(x) := Ax$ and $V_\lambda$ be the eigenspace of $\lambda$.

If $x \in V_\lambda$, then $Ax = \lambda x$ and $ABx = BAx = \lambda Bx$. So $Bx \in V_\lambda$. So $\Phi_B(V_\lambda) \subseteq V_\lambda$. Let $v$ be an eigenvector of $\Phi_B|_{V_\lambda}$. Then $v$ is an eigenvalue for both $A$ and $B$.

Jan 2011 #4

The following matrix has four distinct real eigenvalues. Find their sum and their product.
Jan 2010 #1
Let $A$ be the a $n \times n$ complex matrix which does not have eigenvalue $-1$. Show that the matrix $A + I_n$ is invertible.

Sol: Let $f(t)$ be the characteristic polynomial of $A$. Then $f(-1) \neq 0$. $det(A + I_n) = (-1)^n f(-1) \neq 0$.

Aug 2011 #3
Let $A$ be the $n \times n$ matrix with zeros on the diagonal and ones everywhere else. Find the characteristic polynomial of $A$.

Sol: First observe that $(1, 1, 1, ..., 1)^T$ is an eigenvector corresponding to eigenvalue $n - 1$.

And $(A_n + I_n) = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}$ is rank 1. So null space has dimension $n - 1$. A basis is given by $(1, -1, 0, ..., 0)^T, (1, 0, -1, ..., 0)^T, ..., (1, 0, 0, ..., -1)^T$.

Hence $A_n$ is diagonalizable to $D_n = \begin{bmatrix} n - 1 \\ \vdots \\ -1 \\ \vdots \\ -1 \end{bmatrix}$ and therefore, the characteristic polynomial is $(t - n + 1)(t + 1)^{n-1}$.

To do it directly, let $f_n(t) = det(tI_n - A_n) = t \times f_{n-1}(t) + det \begin{bmatrix} -1 & -1 & -1 & \cdots & -1 \\ -1 & t & -1 & \cdots & -1 \\ -1 & -1 & t & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \cdots & t \end{bmatrix} - det \begin{bmatrix} -1 & -1 & -1 & \cdots & -1 \\ -1 & -1 & -1 & \cdots & -1 \\ -1 & -1 & -1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t + 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$

\[ \therefore f_n(t) = t \times f_{n-1}(t) + (n-1)det \begin{bmatrix} -1 & -1 & -1 & \cdots & -1 \\ -1 & t & -1 & \cdots & -1 \\ -1 & -1 & t & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \cdots & t \end{bmatrix} = t \times f_{n-1}(t) + (n-1)det \begin{bmatrix} -1 & -1 & -1 & \cdots & -1 \\ 0 & t+1 & 0 & \cdots & 0 \\ 0 & 0 & t+1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & t+1 \end{bmatrix} \]

Therefore, $f_n(t) = t \times f_{n-1}(t) - (n-1)(t+1)^{n-2}$.

It can be check that $f_2 = (t-1)(t+1)$, so

\[
\begin{align*}
f_2(t) &= t(t-1)(t+1) - 2(t+1) = (t-2)(t+1)^2 \\
f_2(t) &= t(t-2)(t+1)^2 - 3(t+1)^2 = (t-3)(t+1)^3.
\end{align*}
\]

Using induction, we can see $f_n(t) = (t - n + 1)(t + 1)^{n-1}$.

- Ring Theory
Aug 2011 #6
Let $P$ be a prime ideal in a commutative ring $R$ with 1, and let $f(x) \in R[x]$ be a polynomial of positive degree. Prove that following statement: if all but the leading coefficient of $f(x)$ are in $P$ and $f(x) = g(x)h(x)$, for some non-constant polynomials $g(x), h(x) \in R[x]$, then the constant term $f(0)$ is in $P^2$.

Sol: $f = \tilde{a}_n x^n = \tilde{g}h$. Hence all but the leading coefficient of $\tilde{g}$ are 0 and all but the leading coefficient of $\tilde{h}$ are 0 as $R/P$ is an integral domain. Hence $g(0), h(0) \in P$ and hence $f(0) = g(0)h(0) \in P^2$.

Jan 2011 #7
Prove that in a commutative ring with a finite number of elements, prime ideals are maximal.
Sol: We can show that an integral domain with finite element is a field. Hence the result follows.

Jan 2011 #9
1. Give an example of a ring $R$ and a unit $r \in R$ with $r \neq 1$.
2. Give an example of a ring $R$ and a nilpotent element $r \in R$ with $r \neq 0$.
3. Show that for any ring $R$ and for any element $r \in R$, that $r$ is a nilpotent element of $R$ iff $1 - rx$ is a unit in the polynomial ring $R[x]$.

Sol: $\mathbb{Q}$, 2.
$\mathbb{Z}/4\mathbb{Z}$, 2.
If $r^k = 0$, then $(1 - rx)(1 + rx + r^2x^2 + ... + r^{k-1}x^{k-1}) = 1 - r^kx^k = 1$. If $(1 - rx)(a_0 + a_1x + ... + a_nx^n) = 1$, then $a_0 = 1, a_1 = r, a_2 = r^2, ..., a_n = r^n$. Hence $1 - r^{n+1}x^{r+1} = 1$ implies $r^{n+1} = 0$.

Another way to see it is by:
For all prime ideal $P$, $1 - \tilde{r}x$ is a unit in $R/P[x]$. But $R/P$ is an integral domain. So $\tilde{r} = 0$. Hence $r \in \cap P = \sqrt{0}$.

Aug 2010 #6
Let $R$ be a ring with 1. Define $a \in R$ to be periodic of period $k$ if $a, a^2, a^3, ..., a^k$ are all different, but $a^{k+1} = a$.
1. In $R = \mathbb{Z}/76\mathbb{Z}$, find an element $a \neq 0, 1$ of period 1.
2. In the same ring $R = \mathbb{Z}/76\mathbb{Z}$, find an element that is not periodic.
3. In $R = \mathbb{Z}/76\mathbb{Z}$, list the possible periods and the elements of each period.

Sol: $S = \mathbb{Z}/4\mathbb{Z}$, $T = \mathbb{Z}/19\mathbb{Z}$. So $R \cong S \times T$.
Notice that $r$ is periodic iff $s, t$ are periodic where $\phi(r) = (s, t)$.
0, 1 $\in S$ are elements of period 1 and 0, 1 $\in T$ are elements of period 1.
So 0, 1, 57, 20 are the elements of period 1 of $R$.
Every element in $T$ is periodic and 0, 1, 3 are periodic element in $S$.
So the element that are not periodic are: 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, 66, 70, 74.

<table>
<thead>
<tr>
<th>element in $S$</th>
<th>period</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>element in $S$</th>
<th>period</th>
<th>element in $S$</th>
<th>period</th>
<th>element in $S$</th>
<th>period</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 1</td>
<td>1</td>
<td>14</td>
<td>18</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>18</td>
<td>9</td>
<td>9</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>18</td>
<td>2</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>17</td>
<td>9</td>
<td>10</td>
<td>18</td>
</tr>
<tr>
<td>16</td>
<td>9</td>
<td>15</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>18</td>
<td>11</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>3</td>
<td>18</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

So by $r = \phi^{-1}(s, t) = 20t - 19s$.
## Jan 2010 #12
Determine the following ideals in \( \mathbb{Z} \) by giving generators:
\((2) + (3), (4) + (6), (2) \cap (3), (4) \cap (6)\)
Sol: \(1, 2, 6, 12\).

## Jan 2012 #11
Prove that the rings \( \mathbb{F}_{16}, \mathbb{F}_4 \times \mathbb{F}_4 \), and \( \mathbb{Z}/16\mathbb{Z} \) are pairwise non-isomorphic.
Sol: \( \mathbb{F}_{16} \) has no zero divisor.
\( \mathbb{F}_4 \times \mathbb{F}_4 \) has no element of order >4.
Can use the number of unit element and the number of ideal.

## Aug 2010 #7
In this problem, \( R \) is a finite commutative ring with 1. Let \( p(x) \in R[x] \), the ring of polynomials over \( R \).

1. Show that \( a \in R \) is a root of \( p(x) \) iff \( p(x) \) can be written as \( p(x) = (x - a)g(x) \) with \( g(x) \in R[x] \) of degree one less than the degree of \( g(x) \).

2. Prove or give a counter example: A polynomial of \( p(x) \in R[x] \) of degree \( n \) can have at most \( n \) distinct roots in \( R \).

Sol: Clear for the first part by DA.
\( R = 6\mathbb{Z} / 6\mathbb{Z}, f(x) = (x - 2)(x - 3) = x^2 - 5x = x(x - 5) \).

## Jan 2012 #12 (Jan 2010 #9)
Find all the maximal ideals in \( \mathbb{R}[x] \). (Describe the prime ideals in \( \mathbb{C}[x] \))
Sol: \( \mathbb{R}[x] \) is a PID, and so any prime ideal is generated by an irreducible polynomial. But the irreducible polynomial is either \( x - a \) or \( x^2 - bx + c \) with \( b^2 < 4c \) as \( \mathbb{C} \) is algebraically closed.

## Jan 2010 #13
Let \( f(x) \in \mathbb{C}[x] \) be a polynomial of degree \( n \) such that \( f \) and \( f' \) (the derivative of \( f \)) have no common roots. Show that the quotient ring \( \mathbb{C}[x]/(f) \) is isomorphic to \( \mathbb{C} \times \mathbb{C} \times \ldots \times \mathbb{C}(n \text{ times}) \).
Sol: \( f \) and \( f' \) have no common roots implies that \( f \) has simple root. So \( f(x) = a \prod_{1 \leq i \leq n} (x - c_i) \) where \( c_i \) are distinct.
But then the ideals \((x - c_1), (x - c_2), \ldots, (x - c_n)\) are pairwise comaximal, and hence \( \mathbb{C}[x]/(f) = \mathbb{C}[x]/(x - c_1) \times \mathbb{C}[x]/(x - c_2) \times \ldots \times \mathbb{C}[x]/(x - c_n) = \prod_{1 \leq i \leq n} \mathbb{C}[x]/(x - c_i) = \prod_{1 \leq i \leq n} \mathbb{C} \).

## Aug 2011 #5
Let \( R = \mathbb{K}[x, y, z]/(x^2 - yz) \), where \( \mathbb{K} \) is a field. Show that \( R \) is an integral domain, but not a unique factorization domain.
Sol: First prove \((x^2 - yz) \) is a prime ideal. Since \( \mathbb{K}[x, y, z] \) is an UFD, it suffices to show \( x^2 - yz \) is irreducible.
Suppose \( f, g \in \mathbb{K}[x, y, z] \) s.t. \( fg = x^2 - yz \). Then \( \deg(f) + \deg(g) = 2 \) and hence \( \deg(f) = 0, 1, 2 \).
We need to show \( \deg(f) \neq 1 \).
Otherwise, \( f = ax + by + cz \) and \( g = px + qy + rz \) (no constant term).
\( ap = 1 \), so we may assume, \( a = p = 1 \). Then \( b + q = 0, c + r = 0, bq = 0, cr = 0 \).
Contradiction as \( br + cq = 1 \).
Let \( \bar{x} = \bar{y}z \) be an element in \( R \). We will show this \( \bar{x} \), \( \bar{y} \), \( \bar{z} \) are irreducible but \( \bar{x} \sim \bar{y} \) or \( \bar{y} \sim \bar{z} \).

<table>
<thead>
<tr>
<th>( S \times T )</th>
<th>( R )</th>
<th>period</th>
</tr>
</thead>
<tbody>
<tr>
<td>((0,0),(0,1),(1,0),(1,1))</td>
<td>0,20,57,1</td>
<td>1</td>
</tr>
<tr>
<td>((0,1),(1,1),(3,1),(3,3))</td>
<td>56,37,75,19,39</td>
<td>2</td>
</tr>
<tr>
<td>((3,7),(3,11))</td>
<td>7,11</td>
<td>6</td>
</tr>
<tr>
<td>((0,8),(1,8),(3,8),(0,12),(1,12),(3,12))</td>
<td>8,65,27,12,69,31</td>
<td>6</td>
</tr>
<tr>
<td>((0,4),(0,16),(0,9),(0,17),(0,6),(0,5))</td>
<td>4,16,28,36,44,24</td>
<td>9</td>
</tr>
<tr>
<td>((1,4),(1,16),(1,9),(1,17),(1,6),(1,5))</td>
<td>61,73,9,17,25,5</td>
<td>9</td>
</tr>
<tr>
<td>((3,4),(3,16),(3,9),(3,17),(3,6),(3,5))</td>
<td>23,35,47,55,63,43</td>
<td>18</td>
</tr>
<tr>
<td>((0,2),(0,13),(0,14),(0,15),(0,3),(0,10))</td>
<td>40,32,52,72,60,48</td>
<td>18</td>
</tr>
<tr>
<td>((1,2),(1,13),(1,14),(1,15),(1,3),(1,10))</td>
<td>21,13,33,53,41,29</td>
<td>18</td>
</tr>
<tr>
<td>((3,2),(3,13),(3,14),(3,15),(3,3),(3,10))</td>
<td>39,51,71,13,5,67</td>
<td>18</td>
</tr>
</tbody>
</table>
Suppose $\bar{x} = \bar{f}g$. Choose representative $f, g \in K[x, y, z]$ such that $f$ and $g$ has minimal degree.

Say $f = f_0 + f_1 + \ldots + f_r$ and $g = g_0 + \ldots + g_s$. Then $x^2 - yz|fg - x$. If $r + s > 1$, then $x^2 - yz|fg$ and hence contradict to the minimality of $r$ and $s$.

So $r + s = 1$ and hence one of $f$ and $g$ must be constant. So this prove that $\bar{x}$ is irreducible.

Similarly for $\bar{y}$ and $\bar{z}$.

And finally, it is not hard to see that $\bar{x}$ is not associated to $\bar{y}$.

Aug 2010 #12

For which values of $n$ in $\mathbb{Z}$ does the ring $\mathbb{Z}[x]/(x^3 + nx + 3)$ have no zero divisors?

Sol: It is the same to find the values of $n$ s.t. $x^3 + nx + 3$ is irreducible over $\mathbb{Z}$ as $\mathbb{Z}[x]$ is an UFD. (ref. Michael Artin book, on the section of Gauss lemma.)

Since $x^3 + nx + 3$ is primitive polynomial and then it is reducible iff it has a root in $\mathbb{Q}$ (or $ax + b$ is a factor of $x^3 + nx + 3$ for some relative prime integers $a, b$).

Then $n = 1$ and $n = 3$ implies that the root is either $\pm 1$ or $\pm 3$. Hence $1 + n + 3 = 0$ or $-1 - n + 3 = 0$ or $27 + 3n + 3 = 0$.

Hence $n = -4, 2, -10, -8$ are the value that $x^3 + nx + 3$ is reducible and hence the value that $\mathbb{Z}[x]/(x^3 + nx + 3)$ have zero divisors.

Aug 2010 #11

Let $M$ be the ring of $3 \times 3$ matrices with integer entries. Find all maximal two-sided ideals of $M$.

Sol: If $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \in M$, then $\begin{bmatrix} a & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} d & e & f \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} g & h & i \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in M$ and hence $\begin{bmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \ldots \in M$. So $\begin{bmatrix} gcd(a, b, c, \ldots, i) & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in M$ and hence $M = kM_3 \times 3(\mathbb{Z})$ where $k$ is gcd of all entries of all elements in $M$.

So $M$ is maximal iff $k$ is a prime number.

- Linear Algebra part 2

Jan 2012 #3

Find the eigenvalues and a basis for the eigenspace of the matrix.

$$B = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Sol: Since the matrix is in triangular form, so the eigenvalues are the diagonal entries.

For e.v. $= 1$, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is an eigenvector.

For e.v. $= 0$, $\begin{bmatrix} 2 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 3 & 0 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ forms a basis for the eigenspace.

Jan 2010 #2 (Jan 2012 #1)

Find invertible matrix $P$ s.t. $P^{-1}AP$ is diagonal where

$$A = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$$

Sol: For $A = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, it may be possible to guess $\begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & -1 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & -i & -1 \\ -1 & 1 & -i \end{bmatrix}$, $\begin{bmatrix} 1 & i & -1 \\ -i & 1 & -1 \end{bmatrix}$ are the eigenvector for eigenvalue $1, -1, i, -i$ respectively.

In general, find the characteristic polynomial of $A = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$ first.
\[ \text{char}_A(t) = \det \begin{pmatrix} t & 0 & 0 & -4 \\ -1 & t & 0 & 0 \\ 0 & -2 & t & 0 \\ 0 & 0 & -3 & t \end{pmatrix} = t \times \det \begin{pmatrix} t & 0 \\ -2 & t \end{pmatrix} + 4\det \begin{pmatrix} -1 & t \\ -2 & t \end{pmatrix} \]

\[ = t^4 - 24 = (t - a)(t + a)(t - ia)(t + ia) \text{ where } a = \sqrt{24}. \]

Put \( w = 1 \) (why?), then \( z = a/3, y = a^2/6, x = a^3/6. \)

Put \( w = 1, \) then \( z = -a/3, y = a^2/6, x = -a^3/6. \)

Put \( w = 1, \) then \( z = ia/3, y = -a^2/6, x = -ia^3/6. \)

Put \( w = 1, \) then \( z = -ia/3, y = -a^2/6, x = ia^3/6. \)

There \( \begin{pmatrix} a^3/6 \\ a^2/6 \\ a^3/6 \end{pmatrix}, \begin{pmatrix} -a^3/6 \\ -a^2/6 \\ -ia^3/6 \end{pmatrix}, \begin{pmatrix} ia^3/6 \\ ia/3 \\ 1 \end{pmatrix}, \begin{pmatrix} ia^3/6 \\ ia/3 \\ 1 \end{pmatrix} \) are the eigenvector for the eigenvalue \( a, -a, ia, -ia \) respectively.

Jan 2012 #2

Find the matrix \( A^{2001} \) for \( A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \)

Sol: From the previous example, characteristic polynomial is \( t^4 - 1. \)

So we have \( A^4 = I \) which can be checked directly.

So \( A^{2001} = (A^4)^{500}A = A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \)

Aug 2011 #4

Find the Jordan canonical form of \( \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 4 \end{pmatrix}. \)

Sol: It is clear that the eigenvalues are 1,4,4.

Denote \( A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 4 \end{pmatrix}. \)

\( A - I = \begin{pmatrix} 0 & 2 & 3 \\ 0 & 3 & 5 \\ 0 & 0 & 3 \end{pmatrix}, \) so \( \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \) is an eigenvector.

\( A - 4I = \begin{pmatrix} -3 & 2 & 3 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{pmatrix}, \) so \( \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \) is an eigenvector.
\[(A - 4I)^2 = \begin{bmatrix} -3 & 2 & 3 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} -3 & 2 & 3 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 9 & -6 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \]
so \[\begin{bmatrix} 0 \\ 1 \\ 6 \end{bmatrix}\] is an generalized eigenvector.

So the Jordan canonical form is \[\begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{bmatrix}\].

Jan 2012 #4

Find the matrix \(e^C := I + C + \frac{C^2}{2} + \ldots\) where
\[C = \begin{bmatrix} 1 \\ 4 \\ 1 \\ 1 \end{bmatrix}\]

Sol: \(t^2 - 2t - 3 = (t-3)(t+1)\) is the characteristic polynomial.
\[C - 3I = \begin{bmatrix} -2 & 4 \\ 1 & -2 \end{bmatrix}, \text{ so } \begin{bmatrix} 2 \\ 1 \end{bmatrix}\] is an eigenvector.
\[C + I = \begin{bmatrix} 2 \\ 4 \\ 1 \\ 2 \end{bmatrix}, \text{ so } \begin{bmatrix} -2 \\ 1 \end{bmatrix}\] is an eigenvector.

So \[C = \begin{bmatrix} 2 & -2 \\ 1 & 1 \\ 3 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -\frac{1}{4} & \frac{1}{2} \\ \frac{1}{2} & \frac{3}{4} \end{bmatrix}\].
Hence \[e^C = \begin{bmatrix} 2 & -2 \\ 1 & 1 \\ 0 & e^{-1} \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 1 \\ e^{3} & -e^{-1} \end{bmatrix} \begin{bmatrix} -\frac{1}{4} & \frac{1}{2} \\ \frac{1}{2} & \frac{3}{4} \end{bmatrix} = \begin{bmatrix} e^3 & e^{-1} \\ e^3 & e^{-1} \end{bmatrix} \begin{bmatrix} \frac{e^3 + e^{-1}}{2} \\ \frac{e^3 - e^{-1}}{2} \end{bmatrix}\]

Aug 2010 #9

Let \(A\) be a \(5 \times 5\) real matrix of rank 2 having \(\lambda = -i\) as one of its eigenvalues. Show that \(A^3 = -A\) and that \(A\) is diagonalizable.

Sol: Since \(A\) is real, so \(\bar{\lambda} = i\) is also an eigenvalue. \(A\) has rank 2 implies that null space has dimension 3. or equivalently, there are 3 independent vector for the eigenvalue 0.

Together with the eigenvector of \(i, -i\), there are a basis consists of eigenvectors of \(A\). So \(A\) is diagonalizable.

And the corresponding diagonal matrix is \[\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\].

We also have the minimal polynomial of \(A\) is \(t - (t + i)(t - i) = t^3 + t\). Hence \(A^3 + A = 0\) or \(A^3 = -A\).

Aug 2011 #1

Let \(A\) be a matrix in \(GL_n(C)\). Show that if \(A\) has finite order(i.e. \(A^k\) is the identity matrix for some \(k \geq 1\), then \(A\) is diagonalizable.

Sol: Suppose \(A^k = I\), so \(t^k - 1\) is a multiple of the minimal polynomial.
Notice that \(t^k - 1\) has simple roots: \(\gcd(t^k - 1, kt^{k-1}) = 1\) or \(t^k - 1 = \prod(t - e^{2\pi i/k})\).
So we must have that the minimal polynomial has simple roots.
So \(A\) is diagonalizable.

Jan 2011 #6

A \(5 \times 5\) matrix \(A\) satisfies the equation \((A - 2I)^3(A + 2I)^2 = 0\). Assume that there are at least two linearly independent vectors \(v\) satisfy \(Av = 2v\).

What are the possibilities for the Jordan canonical form?

Sol: \[\begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}\]
Jan 2011 #10

Let $M_n(\mathbb{C})$ denote the vector space over $\mathbb{C}$ of all $n \times n$ complex matrices. Prove that if $M$ is a complex $n \times n$ matrix, then $C(M) = \{A \in M_n(\mathbb{C}) | AM = MA\}$ is a subspace of $M_n(\mathbb{C})$ if dimension at least $n$.

SOL: It is easy to check $C(M)$ is a complex vector space.

Suppose $\mathbb{C}^n = V_1 \oplus V_2 \oplus \ldots \oplus V_k$, s.t. $\Phi_M|_{V_i}$ has Jordan canonical form

\[
\begin{bmatrix}
  a_i & 1 & & \\
  & a_i & 1 & \\
  & & \ddots & \ddots \\
  & & & a_i
\end{bmatrix}
\]

where $a_i$ may not be distinct.

So it is easy to see there are $n_i = \text{dim}(V_i)$ transformation on $V_i$ that commute with $\Phi_M|_{V_i}$ and are independent.

Namely,

\[
\begin{bmatrix}
  1 & & & \\
  & 1 & & \\
  & & \ddots & \\
  & & & 1
\end{bmatrix}
\]

All this can be extend to a transformation of $\mathbb{C}^n$ which is trivial on $V_j$ for $j \neq i$ and is one of the

\[
\begin{bmatrix}
  1 & & & \\
  & 1 & & \\
  & & \ddots & \\
  & & & 1
\end{bmatrix}
\]

Then we see that we at least $n_1 + n_2 + \ldots + n_k = \text{dim}(V_1) + \text{dim}(V_2) + \ldots + \text{dim}(V_k) = n$ independent transformation.

\[ \begin{bmatrix} 2 & 2 \\ 2 & -2 & 1 \\ -2 & 2 & -2 & 2 \\ 2 & -2 & 1 & -2 \\ -2 & 2 & -2 & -2 \end{bmatrix} \]

Jan 2012 #9

Find all irreducible polynomials of degree $\leq 4$ in $\mathbb{F}_2[x]$.

SOL: It is easy to find irreducible polynomial of degree 1,2,3.

Namely, $x, x-1$ are the linear polynomials.

And $x^2 + ax + b$ is irreducible, then $1 + a + b = 1$ and $b = 1$. So $x^2 + x + 1$.

For degree 4, except that 0,1 are not roots and also it is not product of quadratic. (hence $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1$)

For degree 4, except that 0,1 are not roots and also it is not product of quadratic. (hence $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1$)

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

Jan 2012 #10

Find the set of polynomials in $\mathbb{F}_2[x]$ which are the minimal polynomials of elements in $\mathbb{F}_{16}$.

SOL: degree 1,2,4: $x, x-1, x^2 + x + 1, x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1$.

It can be check that the product of these polynomial is $x^{16} - x$.

Aug 2010 #1

Find all irreducible monic quadratic polynomials in $\mathbb{F}_2[x]$.

SOL: $x^2 + ax + b, b \neq 0, 1 + a + b \neq 0, 1 - a + b \neq 0$.

\[ a = 0, b = 1, x^2 + 1 \]

\[ a = 1, b = -1, x^2 + x - 1 \]

\[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \]

ALGEBRAIC NUMBER THEORY
\[ a = -1, b = -1, \ x^2 - x - 1 \]

Jan 2010 #11

1. Prove that the polynomial \( x^2 + x + 1 \) is irreducible over the field \( \mathbb{F}_2 \) with two elements.

2. Factor \( x^9 - x \) into irreducible polynomials in \( \mathbb{F}_3[x] \), where \( \mathbb{F}_3 \) is the field with three elements.

Sol: follows from above.

Jan 2011 #8

Let \( \mathbb{F}_4 \) be the finite field with 4 elements. Express \( \mathbb{F}_4[x]/(x^4 + x^3 + x^2 + 1) \) as a product of fields. Prove your result.

Sol: Is \( x^4 + x^3 + x^2 + 1 \) irreducible?

First we can try the elements in \( \mathbb{F}_4: 0, 1, h, 1 + h = h^2 \)

1 is a root. So \( x^4 + x^3 + x^2 + 1 = (x + 1)(x^3 + x + 1) \).

Since \( x^3 + x + 1 \) has no roots, it is irreducible.

The ideals generated by \( x + 1 \) and \( x^3 + x + 1 \) are comaximal as these two polynomials are relative prime in PID, \( \mathbb{F}_4[x] \).

So by CRT, \( \mathbb{F}_4[x]/(x^4 + x^3 + x^2 + 1) \simeq \mathbb{F}_4[x]/(x + 1) \times \mathbb{F}_4[x]/(x^3 + x + 1) \simeq \mathbb{F}_4 \times \mathbb{F}_{64} \)

Aug 2011 #7

Let \( p \) be a prime number and denote by \( \mathbb{F}_p \) the field with \( p \) elements. For a positive integer \( n \), let \( \mathbb{F}_p^n \) be the splitting field of \( x^{p^n} - x \in \mathbb{F}_p[x] \). Prove that the following are equivalent:

1. \( k|n \)
2. \( (p^k - 1)|(p^n - 1) \)
3. \( \mathbb{F}_{p^k} \subset \mathbb{F}_{p^n} \)

Sol: (1\(\Rightarrow\)2), if \( n = kr \), then \( p^n - 1 = (p^k - 1)(p^{r-1} + p^{r-2} + \ldots + 1) \)

(2\(\Rightarrow\)3), if \( (p^k - 1)|(p^n - 1) \), then \( x^{p^n - 1} - 1 \) are comaximal as these two polynomials are relative prime in PID, \( \mathbb{F}_4[x] \).

(3\(\Rightarrow\)1) If \( \mathbb{F}_{p^k} \subset \mathbb{F}_{p^n} \) then \( \mathbb{F}_{p^n} \) is a \( \mathbb{F}_{p^k} \) vector space \( \simeq (\mathbb{F}_{p^k})^n \). Then by comparing numbers of elements, we have \( p^n = (p^k)^r \) and hence \( n = kr \).

Aug 2010 #4

Is it possible to find a field \( F \) with at most 100 elements so that \( F \) has exactly five different proper subfields? If so, find all such fields. If not, prove that no such field \( F \) exists.

Sol: Finite field has prime power and so the possible power are:

\( 81 = 2^4, 27, 9, 3, 64 = 2^6, 32, 16, 8, 4, 2, 49, 7, 25, 5, \) and some other primes < 100. From the previous problem, we see that no such field exist.

Aug 2011 #8

1. Show that \( x^3 - 2 \) and \( x^5 - 2 \) are irreducible over \( \mathbb{Q} \).

2. How many field homomorphism are there from \( \mathbb{Q}[\sqrt{2}, \sqrt{3}] \) to \( \mathbb{C} \)?

3. Prove that the degree of \( \sqrt{2} + \sqrt{3} \) over \( \mathbb{Q} \) is 15.

Sol: They are Eisenstein polynomials.

There are 15 homomorphisms.

\( \sqrt{2} \mapsto e^{2k\pi i/3} \sqrt{2}, \sqrt{3} \mapsto e^{2k\pi i/5} \sqrt{3} \)

Since 5, 3 are relative prime, \( x^3 - 2 \) remains irreducible over \( \mathbb{Q}[e^{2\pi i/5} \sqrt{2}] \), and hence there are 15 maps

Counter example, \( x^2 + 1, x^4 + 1 \).

Part 3, need to find the minimal polynomial \( f(t) \) over \( \mathbb{Q} \) (either 1, 3, 5, 15)

Conjugates of \( \sqrt{2} + \sqrt{3} \) over \( \mathbb{Q} \) is the roots of the minimal polynomials and at the same time the image of \( \sqrt{2} + \sqrt{3} \) under the any field homomorphism from \( \mathbb{Q}[\sqrt{2} + \sqrt{3}] \) to \( \mathbb{C} \).

To conclude degree of \( f(t) \) is 15, we need to show that \( e^{2k\pi i/3} \sqrt{2} + e^{2k\pi i/5} \sqrt{3} \) are all distinct.
Suppose \( e^{2k\pi i/3} \sqrt[3]{2} + e^{2l\pi i/5} \sqrt[5]{2} = e^{2k\pi i/3} \sqrt[3]{2} + e^{2l\pi i/5} \sqrt[5]{2} \).

Then \( \frac{\sqrt[3]{2}}{\sqrt[5]{2}} = \frac{e^{2k\pi i/3} - e^{2l\pi i/5}}{e^{2k\pi i/3} - e^{2l\pi i/5}} \), but the RHS is in a field of degree 15 over \( \mathbb{Q} \) and LHS is in a field of degree 8 or 4 over \( \mathbb{Q} \). Hence it should be contained in \( \mathbb{Q} \). But this is a contradiction as RHS is a generator of \( \mathbb{Q}[\sqrt[3]{2} + \sqrt[5]{2}] \).

Hence all the \( e^{2k\pi i/3} \sqrt[3]{2} + e^{2l\pi i/5} \sqrt[5]{2} \) are distinct and hence \( \sqrt[3]{2} + \sqrt[5]{2} \) has 15 conjugates.

Jan 2010 #10

Find the degree of the minimal polynomial of \( \alpha = \sqrt[3]{2} + \sqrt[5]{2} \) over \( \mathbb{Q} \).

Sol:

Method 1: Follow the idea of last problem, check \( \pm \sqrt[3]{2} + e^{2k\pi i/3} \sqrt[5]{2} \).

\( 2\sqrt[3]{2} = (e^{2k\pi i/3} - e^{2l\pi i/5}) \sqrt[5]{2} \) can’t be true, so all six conjugate are different.

Method 2: It is clear then \( \mathbb{Q}[\sqrt[3]{2}, \sqrt[5]{2}] : \mathbb{Q} = 6 \) as \( \mathbb{Q}[\sqrt[3]{2}] \) and \( \mathbb{Q}[\sqrt[5]{2}] \) are subfields of degree 2,3 over \( \mathbb{Q} \).

Claim: \( \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[\sqrt[3]{2} + \sqrt[5]{2}] \).

Suppose \( \alpha = \sqrt[3]{2} + \sqrt[5]{2} \) is irreducible and hence does not have common root and hence \( \alpha \) can not be a root for both polynomial.

Hence \( \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[\sqrt[3]{2} + \sqrt[5]{2}] \).

Then \( \alpha - \sqrt[3]{2} = \sqrt[5]{2} \in \mathbb{Q}[\sqrt[3]{2} + \sqrt[5]{2}] \) implies that \( \mathbb{Q}[\sqrt[3]{2} + \sqrt[5]{2}] = \mathbb{Q}[\sqrt[3]{2}, \sqrt[5]{2}] \) and so the extension is of degree 6.

Method 3: Let \( \alpha = \sqrt[3]{2}, b = \sqrt[5]{2} \). Then \( 1, a, ab, ab^2, ab^3 \) are basis of \( \mathbb{Q}[a, b] \)

\((a + b)^3 = 2 + 2ab + b^2, (a + b)^5 = 4a + 2ab + 2ab^2 + 6a + 15ab + 3b^2 \) are Eisenstein, so they are irreducible and hence they does not have common root and hence \( \alpha \) can not be a root for both polynomial.

Hence \( \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[\sqrt[3]{2} + \sqrt[5]{2}] \).

Remark: \( (x - \sqrt[3]{2})^3 = 3 \) hence \( x^3 - 3\sqrt[3]{2}x^2 + 6x - 2\sqrt[3]{2} - 3 = 0 \).

Hence \( x^3 - 6x^2 + 6x + 9 = 18x^3 + 24x^2 + 8 \)
\( x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1 = 0 \) is minimal polynomial of \( \alpha \).

Aug 2010 #10

1. Give an example of an irreducible monic polynomial of degree 4 in \( \mathbb{Z}[x] \) that is reducible in the field \( \mathbb{Q}[\sqrt{2}] \).

Explain why your example has the stated property.

2. Show that there are no irreducible monic polynomial of degree 5 in \( \mathbb{Z}[x] \) that is reducible in the field \( \mathbb{Q}[\sqrt{2}] \).

Sol: \( x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) \) Eisenstein polynomial.

Suppose \( f(x) = g(x)h(x) \) where \( g(x) \) is monic irreducible over \( \mathbb{Q}[\sqrt{2}] \).

Since \( f \) is irreducible over \( \mathbb{Z} \) (hence irreducible over \( \mathbb{Q} \)), so \( g(x) \) has some of the coefficient of the form \( a + b\sqrt{2} \) with \( b \neq 0 \).

Let \( \sigma \) be the automorphism of \( \mathbb{Q}[\sqrt{2}] \) that sends \( \sqrt{2} \) to \(-\sqrt{2} \) and preserve \( \mathbb{Q} \). Then \( f = \sigma(f) = \sigma(g)\sigma(h) \).

It is clear that \( g \) and \( \sigma(g) \) are relative prime in \( \mathbb{Q}[\sqrt{2}][x] \) as they are irreducible and not different but a constant.

So \( g \times \sigma(g)f \). But it is easy to check that \( g \times \sigma(g) \) is in \( \mathbb{Q}[x] \) and of even degree. This implies that \( f \) is reducible over \( \mathbb{Q} \).

Jan 2012 #13

Let \( R = \mathbb{Z}[i] \) and \( I \subset R \) be an ideal. If \( R/I \) has 4 elements what are the possibilities for \( I \) and \( R/I \).

Sol: Let \( J = I \cap \mathbb{Z} \). Then \( \mathbb{Z}/J \hookrightarrow R/I \).

Since \( R/I \) has 4 element, then \( \mathbb{Z}/J \) can have 2,3,4 elements.

Case "3", it is not possible as \( \mathbb{Z}/3\mathbb{Z} \) is a field and hence \( R/I \) is \( \mathbb{Z}/3\mathbb{Z}\)-vector space and hence \( |R/I| \) is a power of 3.

Case "4", then \( \mathbb{Z}/J \cong \mathbb{Z}/4\mathbb{Z} \). So \( J = 4\mathbb{Z} \subset I \).

So \( \mathbb{Z}/J \hookrightarrow R/4R \hookrightarrow \mathbb{Z}/4\mathbb{Z} \).

Now \( R/4R = \mathbb{Z}/4\mathbb{Z} + i\mathbb{Z}/4\mathbb{Z} \)

We will see there are no ideal of 4 elements that does not contain 1,2,3.
So the ideal \( I/4R \) which does not contain 1,2,3 can only have element 0, \( 2 + 2i \), but then \( R/I = (R/4R)/(I/4R) \) has 8 elements.

Therefore, we conclude that \( J = 4\mathbb{Z} \) is not possible.

Case “2”, then \( J = 2\mathbb{Z} \) and hence \( 2 \in I \)

So \( R/2R \to R/I \). But \( R/2R = \mathbb{Z}/2\mathbb{Z} + i\mathbb{Z}/2\mathbb{Z} \) has 4 elements. So we can conclude \( I = 2\mathbb{Z} \) and \( R/I = (\mathbb{Z}/2\mathbb{Z})[i] \).