August 2005
Algebra Qualifying Exam
Solutions

1A) Find all matrices $A \in M_2(\mathbb{R})$ such that $A^4 - A^2 = 12I_2$, where $I_2 \in M_2(\mathbb{R})$ is the identity matrix.
Answer: We know that A satisfies $x^4 - x^2 - 12I = 0$. Thus $(x^2-4)(x^2+3) = (x+2)(x-2)(x^2+3) = 0$. Consider that the minimal polynomial of A must divide one of these. The choices are (up to similarity)

$$\begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 3 & 0 \end{bmatrix}$$

1B) If $A = \begin{bmatrix} 13 & -18 \\ 6 & -8 \end{bmatrix}$ find four square roots B for A (i.e. matrices B with $B^2 = A$).
Answer: We first try to diagonalize the matrix to make easier. We compute the characteristic polynomial

$$\det(A - xI) = x^2 - 5x + 4 = (x-4)(x-1)$$

and so we have eigenvalues $\lambda_1 = 1$ and $\lambda_2 = 4$. Thus we need the corresponding matrix of eigenvalues to diagonalize A.

$$\begin{pmatrix} 12 & -18 \\ 6 & -9 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ and}$$
$$\begin{pmatrix} 9 & -18 \\ 6 & -12 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

has basis for solution of $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$. For $\lambda_2 = 4$ we have $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$. Thus we have that $P^{-1} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ and $P = \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix}$. Thus we have $A = P^{-1}DP$ where $D = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$. We find a square root of D as $C = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 2 \end{pmatrix}$ and so $(P^{-1}CP)^2 = P^{-1}C^2P = P^{-1}DP = A$. So the for choices are the four choices of $P^{-1}CP$.

$$\text{Check} : \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix} = \begin{pmatrix} 3 & 8 \\ 2 & 4 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix}$$
$$= \begin{pmatrix} 13 & -18 \\ 6 & -8 \end{pmatrix}$$

2A) Suppose that G is a group and that given any x, y, and z in G then at least two of them commute with each other. Show that G is abelian.
Answer: Given x, y, z we know that either $xy = yx$, $xz = zx$ or $yz = zy$. Now we need to show given arbitrary $a, b \in G$ that $ab = ba$. We know that for $a, b, ab \in G$ that at least two of them commute. If a and b commute then we are done. If not assume that a commutes with ab. Then $aab = aba$ and thus $a^{-1}aab = a^{-1}aba \implies ab = ba$. If b commutes with ab then $bab = bba \implies b^{-1}bab = b^{-1}bba \implies ab = ba$.

2B) Let G be a simple group of order $12p^n$, where p is a prime and $n \in \mathbb{N}$. Show that G has order 60.

Answer: $12p^n = 2^2 \cdot 3 \cdot p^n$.

Fact: Let G be a group whose order is equal to a product mp^k, where $k > 0$, m is coprime to p and $m < p$. Then G has a normal subgroup of order p.

Proof: Consider the number n_p of Sylow p-subgroups. Then n_p must divide mp^k and it is coprime to p. Thus $n_p | m$. But as n_p is congruent to 1 mod p, if $n_p \neq 1$ then $n_p \geq p+1 > m$, impossible. Thus $n_p = 1$ and the unique Sylow p-subgroup P is in fact normal.

Case (i): $p \neq 3$ as $2 < 3$ and $(2, 3) = 1$ so use fact above.

Case (ii): If $p = 2$ then $12p^n = 2^m \cdot 3$. Thus the number of Sylow 2-subgroups, $n_2 = 1$ or 3. If it is 1 then the subgroup is normal and not a simple group. If $n_2 = 3$ then we have an action of G (by conjugation) on the three 2-Sylow subgroups. Thus we have a homomorphism

$$\varphi : G \to S_3$$

as we are permuting the three 2-Sylow subgroups. But as $|G| > 2^2 \cdot 3 = 12 > 6$ we must have a nontrivial kernel for φ. Thus it is a normal subgroup. Thus $p \neq 2$.

Case (iii) $p > 5$. Thus $|G| = 2^2 \cdot 3 \cdot p$. Thus there are $1, p+1, 2p+1, ...$ Sylow p-subgroups. But as $p > 5$ we know that $p \geq 7$ and so $p+1 \geq 8$. Thus there is only one p-Sylow subgroup and so it is unique.

Case (iv) $p = 5$. Thus $|G| = 60$ and we know that A_5 is a simple group.

3A) Decompose the group algebra $\mathbb{F}_5 S_3$ and $\mathbb{F}_5 \mathbb{Z}_7$ into products of simple rings.

Answer: We know that $\mathbb{F}_5 S_3$ is a semisimple ring by Maschke's theorem. We also know that it is finite and thus it Artinian. As a ring, it is nonabelian as the group S_3 is nonabelian. We know that the order of the ring $\mathbb{F}_5 S_3 = 5^6$ and thus we have that $\mathbb{F}_5 S_3$ is isomorphic to (by the Weddeburn-Artin structure theorem) to

$$M_2(\mathbb{F}_5) \times \mathbb{F}_5 \times \mathbb{F}_5$$

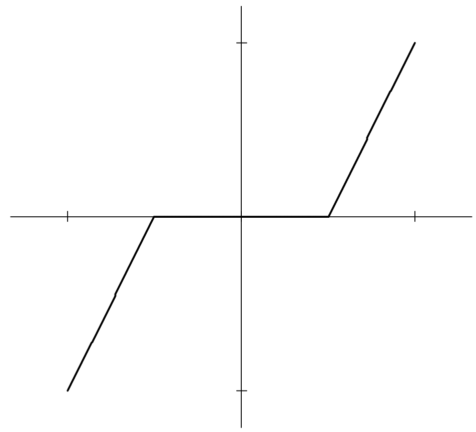
Now we consider $\mathbb{F}_7 \mathbb{Z}_7$. This is a commutative ring as $\mathbb{Z}_7$ is an abelian group. The ring has order 7^7 and is isomorphic to $\mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7 \times \mathbb{F}_7$. This is true because for all abelian groups we have that all representations are 1-dimensional.

3B) Let $R = C[-1, 1]$, the ring of all continuous (real) operatornametions on the interval $[-1, 1]$, with pointwise operations. Define

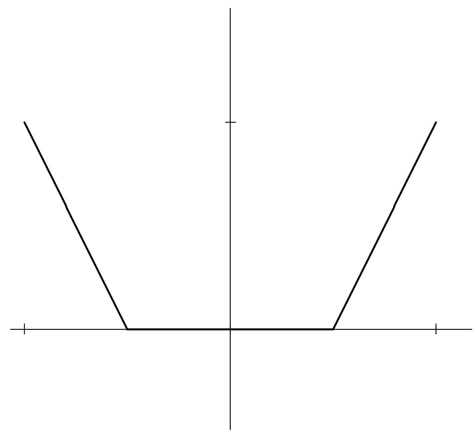
$$f(x) = \left\{ \begin{array}{l} 2x+1, \text{ if } -1 \leq x \leq -1/2 \\ 0, \text{ if } -1/2 \leq x \leq 1/2, \\ 2x-1, \text{ if } 1/2 \leq x \leq 1. \end{array} \right\}$$

and $g(x) = |f(x)|$, so $f, g \in R$. Show that $f|g$ and $g|f$ in R, but that there is no unit $u \in R$ with $g = uf$. (Pictures will be useful).

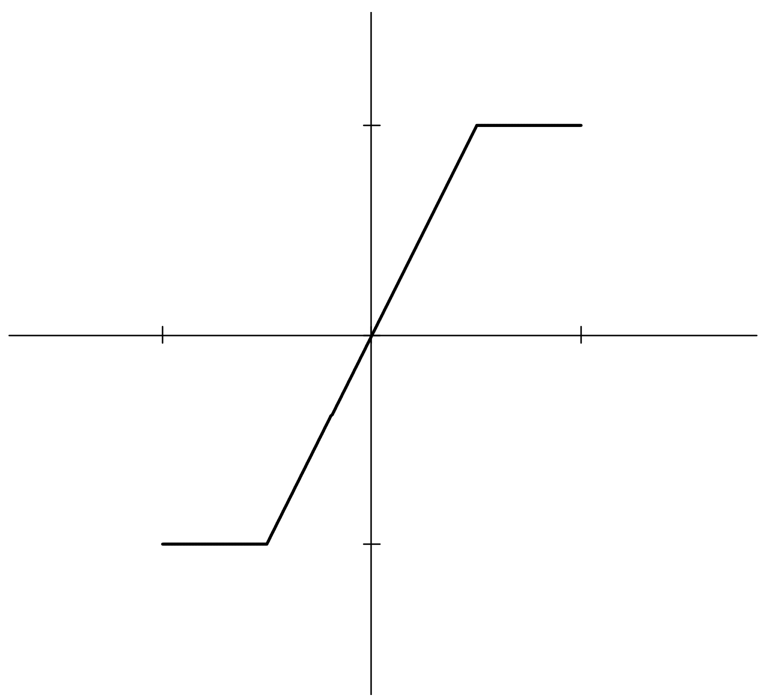
Answer:



and $g(x)$ is



If we let $h(x) =$



then we see that $f(x) = g(x)\,h(x)$ and $g(x) = f(x)\,h(x)$ however the only units in $C[-1,1]$ are the constant functions and $f(x)$ and $g(x)$ are clearly not scalar multiples.

4A) Show that $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ is not solvable by radicals.
Answer: First we note that $f(x)$ is irreducible by the Eisenstein criterion with $p = 5$. Thus we know that $Gal(f(x)) \leq S_5$, a transitive subgroup of the symmetric group on 5 letters. We also note that $f'(x) = 10x^4 - 10$ and thus $f'(x) = 10(x^2-1)(x^2+1)$ and thus $f'(1) = f'(-1) = 0$. We also have that $f''(x) = 40x^3$. Thus at -1 we have a relative max and at 1 a relative min. $f(0) = 5$, $f(-2) = -64 + 20 + 5 < 0$, $f(-1) = -2 + 10 + 5 > 0$, $f(1) = 2 - 10 + 5 < 0$ and $f(2) > 0$. Thus we have 3 real roots and 2 complex (nonreal) roots. We know that there is a 5-cycle as the action of the Galois group on the roots is transitive. We also have a 2-cycle. Thus we can generate S_5 from these two actions. Thus $G \cong S_5$ which is not solvable as it has A_5 as a an index 2 subgroup which is simple.

4B) Let p be a rpime. Let d, m, and $n \in \mathbb{N}$. Let $f(x) \in \mathbb{F}_{p^m}[x]$ be a monic, irreducible polynomial over $\mathbb{F}_{p^m}$ of degree d. Show that $f(x)$ is an irreducible polynomial over $\mathbb{F}_{p^{mn}}$ if and only if g.c.d.$\{n, d\} = 1$.
Answer:

5A) Compute the elementary divisors and the invariant factors of the $\mathbb{F}_3[x]$-module $M := \mathbb{F}_3[x]/(f(x))$, where $f(x) := (x^2+\bar{1})^2(x^2+\bar{2})^2(x^3+x^2+x+\bar{1})^2$. We recall that $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ is the field with 3 elements.
Answer: The invariant factors are $(x^2+\bar{1})^2(x^2+\bar{2})^2(x^3+x^2+x+\bar{1})^2$ and the elementary divisors are $(x^2+\bar{1})^2$, $(x^2+\bar{2})^2$, and $(x^3+x^2+x+\bar{1})^2$. ?????? I think ??????

5B) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ are isomorhic as $\mathbb{Q}$-modules.
Answer: First we note that $\frac{a}{b} \otimes \frac{c}{d} = 1 \otimes \frac{ac}{bd} \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$. Thus any element of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ can be written as $1 \otimes \frac{p}{q}$. Consider the map $\varphi : 1 \otimes \frac{p}{q} \longmapsto 1 \otimes \frac{p}{q}$. First we show this is a $\mathbb{Q}$-module homomorphism.

$$\begin{aligned}
\varphi\left(1 \otimes \frac{p}{q} + 1 \otimes \frac{r}{s}\right) &= \varphi\left(1 \otimes \frac{p}{q} + \frac{r}{s}\right) = 1 \otimes \frac{p}{q} + \frac{r}{s} \\
&= \varphi\left(1 \otimes \frac{p}{q}\right) + \varphi\left(1 \otimes \frac{r}{s}\right) \\
\varphi\left(a \cdot 1 \otimes \frac{p}{q}\right) &= \varphi\left(1 \otimes a\frac{p}{q}\right) = 1 \otimes a\frac{p}{q} \\
&= a\left(1 \otimes \frac{p}{q}\right) = a\varphi\left(1 \otimes \frac{p}{q}\right)
\end{aligned}$$

The map is clearly onto as any element in $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ can be written as $1 \otimes \frac{p}{q}$. For one-to-one assume that $1 \otimes \frac{p}{q} = 1 \otimes \frac{r}{s} \implies 1 \otimes \left(\frac{p}{q} - \frac{r}{s}\right) = 0$ and this implies that $\frac{p}{q} = \frac{r}{s}$. Another way to consider this is to show that they are both isomorphic to $\mathbb{Q}$ as done in a prior qual.