Solution to the final exam in MAT2200 Spring 2007

Exercise 1

1a). Since G is given to be a subring of $M_2(\mathbb{Z}_3)$, to prove that it is a field we need to verify that the multiplication is commutative and that every element different from the zero matrix (which is the additive identity) is invertible for multiplication. For two matrices

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{and } C = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

in G, just compute AC and CA, and see that they are the same because $\mathbb{Z}_3$ is commutative. Now take A as above different from the zero matrix, so a and b are not both equal to 0 in $\mathbb{Z}_3$. We compute that $\det(A) = a^2 + b^2$. Since a and b take values in $\mathbb{Z}_3$, we verify that $a^2 + b^2$ is always different from 0 when a and b are not simultaneously 0. Note that since $\mathbb{Z}_3$ is a field, the non-zero element $a^2 + b^2$ has an inverse $(a^2 + b^2)^{-1}$ in $\mathbb{Z}_3$. Therefore the matrix

$$A^{-1} = (a^2 + b^2)^{-1} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

is in G and is the inverse of A. Thus we've proved that every non-zero element in G is a unit.

1b. Since x^2+1 is of degree 2, it will be reducible over $\mathbb{Z}_3$ only if it has a zero in $\mathbb{Z}_3$. We check all possibilities for a zero (we use the evaluation homomorphism): $\phi_0(x^2 + 1) = 1$, $\phi_1(x^2 + 1) = 2$, $\phi_2(x^2 + 1) = 5 (\mathrm{mod}\, 3) = 2$, so there is no zero in $\mathbb{Z}_3$ and the polynomial is irreducible over $\mathbb{Z}_3$. It follows that the ideal $\langle x^2 + 1\rangle$ is maximal in $\mathbb{Z}_3[x]$. Since $\mathbb{Z}_3[x]$ is a commutative ring, the quotient ring $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ becomes a field.

1c). Here you must verify directly that ϕ is a homomorphism for addition and multiplication. For multiplication you need to note that in the field $\mathbb{Z}_3(\alpha)$ we have $\alpha^2 + 1 = 0$. To prove that ϕ is injective, take a matrix A as above with $\phi(A) = 0$. Then $a + \alpha b = 0$ in $\mathbb{Z}_3(\alpha)$, and since $\{1, \alpha\}$ is a linearly independent set in $\mathbb{Z}_3(\alpha)$ we get $a = b = 0$ in $\mathbb{Z}_3$. Thus $A = 0$ and hence $\ker(\phi) = \{0\}$. To prove surjectivity, you need to note that every element of $\mathbb{Z}_3(\alpha)$ has the form $a + \alpha b$ for some $a, b \in \mathbb{Z}_3$.

Exercise 2

2a). The polynomial $x^5 - 2$ is irreducible by Eisenstein's criterion with $p = 2$ (here you need to give details: p divides all coefficients except the coefficient of the highest degree term, and p^2 does not divide the constant term).

2b). The zeros of $f(x)$ are $\sqrt[5]{2}\zeta^j$ for $j = 0, \ldots, 4$. If we let L denote the splitting field of $f(x)$, then by definition this is the smallest subfield of $\overline{\mathbb{Q}}$ containing these zeros. We have $\sqrt[5]{2}$ and $\sqrt[5]{2}\zeta$ are in L, and since L is a field we also have $\zeta \in L$. Hence $K \leq L$. But K is also a subfield of $\overline{\mathbb{Q}}$ which contains the zeros of $f(x)$ over $\mathbb{Q}$ (because products of elements in K are again in K). Therefore $K = L$. To find the degree of K over $\mathbb{Q}$ we consider the intermediate extensions

$$\mathbb{Q} \leq \mathbb{Q}(\zeta) \leq K \quad \text{and} \quad \mathbb{Q} \leq \mathbb{Q}(\sqrt[5]{2}) \leq K.$$

The first one gives $[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}]$ and the second gives $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[5]{2})][\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}]$. Since the irreducible polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}(\zeta)$ must divide $x^5 - 2$, it has degree at most 5, and since the cyclotomic extension $\mathbb{Q}(\zeta)$ has degree 4 over $\mathbb{Q}$, we see from the first equality that $[K : \mathbb{Q}] \leq 20$ and $[K : \mathbb{Q}]$ is divisible by 4. Similar arguments using the second equality above show that $[K : \mathbb{Q}]$ is also divisible by 5. Hence $[K : \mathbb{Q}] = 20$.

2c). By the main theorem of Galois theory there is a bijective correspondence between intermediate subfields K' with $\mathbb{Q} \leq K' \leq K$ and subgroups of $G(K/\mathbb{Q})$: the subgroup corresponding to K' is $G(K/K')$ and the index $(G(K/\mathbb{Q}) : G(K/K'))$ is equal to $[K' : \mathbb{Q}] = 4$. Now K is a splitting field and a separable extension (because the base field $\mathbb{Q}$ is perfect), and so $|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = 20$. By Sylow's third theorem, the number N of Sylow 5-subgroups is congruent to 1 modulo 5 and divides 20. The only possibility is $N = 1$. Hence $G(K/\mathbb{Q})$ has only one subgroup of order 5. By Sylow's second theorem this subgroup is normal and therefore corresponds to a unique normal intermediate subfield K'. (In fact since $\mathbb{Q}(\zeta)$ has degree 4 over $\mathbb{Q}$ we have $K' = \mathbb{Q}(\zeta)$).

2d). By Sylow's third theorem, the number M of Sylow 2-subgroups is congruent to 1 modulo 2 and divides 20. There are two possibilities, $M = 1$ or $M = 5$. By the main theorem of Galois theory, the Sylow 2-subgroups of $G(K/\mathbb{Q})$ correspond to subfields $\mathbb{Q} \leq E \leq K$ with $[E : \mathbb{Q}] = 5$, and there are either 1 or 5 such subfields. Since $\mathbb{Q}(\sqrt[5]{2}\zeta^j)$ for $j = 0, \ldots, 4$ are such subfields and since for $j = 0$ we have a subfield of $\mathbb{R}$ but for $j = 1, \ldots, 4$ we have a subfield of $\mathbb{C}$, these subfields cannot be all equal. Hence $M = 5$.

Exercise 3

3a). By taking square powers one finds that α is a zero of $f(x) = x^4 - 10x^2 + 5$. By Eisenstein's criterion with $p = 5$ this polynomial is irreducible over $\mathbb{Q}$.

3b). The zeros of $f(x)$ are $\pm\alpha$, $\beta := \sqrt{5 + 2\sqrt{5}}$ and $-\beta$. Since $\alpha\beta = \sqrt{5} = (5 - \alpha^2)/2$, it follows that $\beta \in \mathbb{Q}(\alpha)$ and so $K = \mathbb{Q}(\alpha)$. Therefore $[K : \mathbb{Q}] = \deg(\alpha, \mathbb{Q}) = 4$. Since $\mathbb{Q} \leq \mathbb{Q}(\sqrt{5}) \leq K$ we obtain the second equality from $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$.

3c). Note that K is a normal extension over $\mathbb{Q}$ and so $|G(K/\mathbb{Q})| = 4$. The non-trivial element in $G(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ is the conjugation automorphism $\sigma : \sqrt{5} \mapsto -\sqrt{5}$. The extensions of this to elements in $G(K/\mathbb{Q})$ must send α to either β (call this τ_1) or $-\beta$ (call this τ_2). Then

$$\tau_1(\beta) = \tau_1(\sqrt{5})\tau_1(\alpha)^{-1} = -\sqrt{5}\beta^{-1} = -\alpha$$

and we compute that τ_1 is an element of order 4 in $G(K/\mathbb{Q})$ (for example $\tau_1^4(\alpha) = \tau_1(\tau_1^3(\alpha)) = \tau_1(-\beta) = \alpha$.)