Answers to exam problems, MAT2200, spring 2010

Note: at the exam full details of proofs are required.

Problem 1. For (a), verify that for two elements X, Y in R, their sum and product has again a form which ensures it is in R. For example, if X has a on the diagonal and Y has a' on the diagonal, XY has aa' on the diagonal. The zero matrix is the additive identity. For the existence of additive inverses, take an X in R. Then $-X$ is the matrix with $-a$ on diagonal, and b, c replaced by $-b$ and $-c$, respectively. Since $aa' = a'a$ in $\mathbb{Z}_5$, we have $XY = YX$, so the ring is commutative. The unity is the identity matrix I_3 in $M_3(\mathbb{Z}_5)$ (corresponds to the choice $a = 1$, $b = c = 0$).

For (b), take as before $X, Y \in R$. The map ϕ depends only on the diagonal entries, so suppose X has a on the diagonal and Y has a'. The sum $X + Y$ has $a + a'$ on the diagonal, so $\phi(X + Y) = a + a'$ by definition of ϕ, and this is equal to $\phi(X) + \phi(Y)$ in $\mathbb{Z}_5$. Similarly $\phi(XY) = \phi(X)\phi(Y)$.

For (c), either notice directly that for $X \in R$ and $A \in R$ the products XA and AX have zero on the diagonal, so they belong to I, or note that $I = \ker \phi$, and since the kernel of a ring homomorphism is an ideal we get the first claim. To prove that R/I is a field, note that by the fundamental homomorphism theorem there is an isomorphism $\mu : R/I \to \phi[R]$. We claim ϕ is surjective: let $a \in \mathbb{Z}_5$. Put X the matrix in R with a on diagonal and zero in all other places. Then $\phi(X) = a$. Therefore $\phi[R] = \mathbb{Z}_5$ and we see that R/I is isomorphic to a field with five elements.

Problem 2. (a) Let N_p denote the number of Sylow p-subgroups of G for $p \in \{5, 7, 17\}$. By Sylow's third theorem, $N_p \equiv 1 \pmod p$ and N_p divides $|G| = 5 \cdot 7 \cdot 17$. The possible divisors of $|G|$ (less than $|G|$)are $1, 5, 7, 17, 35, 85, 119$. Now N_{17} is of form $17k+1$ with $k \in \mathbb{Z}^+ \cup \{0\}$, and we get the possibilities $N_{17} \in \{1, 35\}$. Similarly, N_5 is of form $5k + 1$ and we get $N_5 = 1$, and for $N_7 = 7k + 1$ we see that $N_7 \in \{1, 85\}$.

For (b), let K be the Sylow 5-subgroup, and let $g \in G$. Then gKg^{-1} is again a Sylow 5-subgroup. Thus $N_5 = 1$ implies that $gKg^{-1} = K$ so K is normal. To finish, we must show that we cannot have $N_7 = 85$ and $N_{17} = 35$.

Assume that $N_7 = 85$ and $N_{17} = 35$. Let P_i, $i = 1, \ldots, 35$ be the Sylow 17-subgroups, and Q_i, $i = 1, \ldots, 85$ the Sylow 7-subgroups. For $i \neq j$, $P_i \cap P_j$ is a proper subgroup of P_i, so is trivial. Thus there are 35×16 elements of order 17 in G. Similarly there are 6×85 elements of order 7 in G, in all at least 1070 elements, a contradiction. So at least one of $N_7 = 1$ and $N_{17} = 1$ is true.

(c) Since G/K has order 7×17 (by theorem of Lagrange), and since 17 is not congruent to 1 modulo 7, we use the argument of theorem 37.7 to conclude that G/K is cyclic and therefore abelian. First we see as in part (a) that G/K has a Sylow 7-subgroup, call it P, and a Sylow 17-subgroup, call it Q. Then we claim that $P \cap Q = \{e\}$, where e is the identity in G/K. To prove the claim, note that an element $g \in P \cap Q$ will generate a subgroup of order dividing $7 \cdot 17$. If the order is 7, the subgroup must be equal to P, but then $P \subset Q$ which is false (the order of P does not divide the order of Q). Similarly the subgroup cannot have order 17. The claim follows. Next, the map $\phi : P \times Q \to G/K$, $\phi(a, b) = ab$ is a homomorphism because $aba^{-1}b^{-1} \in P \cap Q$ by normality of both subgroups, so $ab = ba$ and so $\phi((a, b)(a', b')) = aa'bb' = aba'b' = \phi(a, b)\phi(a', b')$. Finally, ϕ is injective (its kernel is $P \cap Q$) and surjective ($\phi(P \times Q)$ is a subgroup of G/K containing both P and Q.) Hence ϕ is an isomorphism. Now $P \cong \mathbb{Z}_7$ and $Q \cong \mathbb{Z}_{17}$, so G/K is cyclic and therefore abelian.

Problem 3. (a) $f(x)$ is irreducible by Eisenstein's criterion with $p = 3$. For $g(x)$, the divisors of -3 are $\pm 1, \pm 3$, and we verify that none of them is a zero for $g(x)$. So we look for a factorisation of $g(x)$ into two terms of order 2. Let $g_1(t) = t^2 - 2t - 3$. This has zeros -1 and 3 (either by verifying the divisors of 3 or by using the formula for $t^2 - 2t - 3 = 0$). So $g_1(t) = (t + 1)(t - 3)$. Then $g(x) = g_1(x^2) = (x^2 + 1)(x^2 - 3)$ is the factorisation of $g(x)$ over $\mathbb{Q}$.

For (b) note that we have the extensions

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt{3})(i).$$

Here $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Since $i \notin \mathbb{Q}(\sqrt{3})$ because $\mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$, we have $[\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})] = 2$ (the irreducible polynomial of i over $\mathbb{Q}(\sqrt{3})$ is $x^2 + 1$). In all with $E = \mathbb{Q}(\sqrt{3})(i)$ we have $[E : \mathbb{Q}] = 4$. To find $G(E/\mathbb{Q})$, note that $G(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$ consists of two elements, namely the identity automorphism $\mathrm{id}_{\mathbb{Q}(\sqrt{3})}$, and the conjugation automorphism $\psi_{\sqrt{3},-\sqrt{3}}$. The automorphism $\mathrm{id}_{\mathbb{Q}(\sqrt{3})}$ has only two extensions to automorphisms of E which fix $\mathbb{Q}(\sqrt{3})$, one is the identity automorphism id_E, the second is the automorphism σ_1 which conjugates i onto $-i$. Thus on an arbitrary element in E, expressed as a linear combination of the basis $\{1, \sqrt{3}, i, i\sqrt{3}\}$ we have

$$\sigma_1(a_0 + a_1\sqrt{3} + a_2 i + a_3 i\sqrt{3}) = a_0 + a_1\sqrt{3} - a_2 i - a_3 i\sqrt{3},$$

where $a_j \in \mathbb{Q}$, $j = 0, \ldots, 3$. The extensions of $\psi_{\sqrt{3},-\sqrt{3}}$ to E are the automorphism σ_2 which fixes i, and the automorphism σ_3 which conjugates i onto $-i$. There are no other possibilities of assigning values to the elements $\sqrt{3}$ and i to get automorphisms, so $G(E/\mathbb{Q}) =$

$\{\mathrm{id}_E, \sigma_1, \sigma_2, \sigma_3\}$. Since

$$\sigma_1^2(a_0+a_1\sqrt{3}+a_2 i+a_3 i\sqrt{3}) = \sigma(a_0+a_1\sqrt{3}-a_2 i-a_3 i\sqrt{3}) = a_0+a_1\sqrt{3}+a_2 i+a_3 i\sqrt{3},$$

we have $\sigma_1^2 = \mathrm{id}_E$. Since also

$$\sigma_3^2(a_0+a_1\sqrt{3}+a_2 i+a_3 i\sqrt{3}) = \sigma_3(a_0-a_1\sqrt{3}-a_2 i+a_3 i\sqrt{3}) = a_0+a_1\sqrt{3}+a_2 i+a_3 i\sqrt{3},$$

we have two elements of order 2, so $G(E/\mathbb{Q})$ is isomorphic to the Klein group.

For (c), the splitting field of $\{f(x), g(x)\}$ is the smallest subfield (of $\mathbb{C}$) containing $\mathbb{Q}$ and the zeros in $\mathbb{C}$ of the two polynomials. The zeros of $f(x)$ are $\sqrt[3]{3}$, which is real, and $\sqrt[3]{3}\frac{-1\pm i\sqrt{3}}{2}$ in $\mathbb{C}$. It follows that $K = \mathbb{Q}(\sqrt{3}, i, \sqrt[3]{3})$. We have

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{3})(i) \leq \mathbb{Q}(\sqrt{3}, i, \sqrt[3]{3}).$$

We have $[K : E] = 3$ because the degree of $\sqrt[3]{3}$ over $\mathbb{Q}$ is 3, and therefore $\sqrt[3]{3}$ does not belong to E. In all $[K : \mathbb{Q}] = 12$.