Suggested answers to exam problems, MAT2200, spring 2012

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

Problem 1. For (a), verify the group axioms. The order of G is $(p-1)^2p$, corresponding to all possible values of the entries a, b, c.

For (b), we have $|G| = 12$. Let N_p denote the number of Sylow p-subgroups of G for $p \in \{2, 3\}$. By Sylow's third theorem, $N_p \equiv 1 \pmod p$ and N_p divides $|G| = 12$. Thus N_2 is 1 or 3, and N_3 is 1 or 4. Now, a Sylow 2-subgroup intersects a Sylow 3-subgroup only at identity e (compare order of elements). If $N_3 = 4$ it follows that G must have 8 non-trivial elements of order 3, and so there are three non-trivial elements of order 2 or 4. Hence $N_4 = 1$, and the Sylow 4-subgroup is normal. In case $N_3 = 1$ the Sylow 3-subgroup is normal.

For (c), note that $hk = kh$ for all h, k is equivalent to $hkh^{-1}k^{-1} = e$ for all h, k, and this identity follows from the fact that $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{e\}$. From this the homomorphism claim can be verified. Injectivity follows because $H \cap K = \{e\}$, and surjectivity because $H \times K$ has same cardinality as G. Up to isomorphism, G' is $\mathbb{Z}_4 \times \mathbb{Z}_3$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

For (d), write $K = \{e, k, k^2\}$ for $k \neq e$. Since K is normal in G', we have $hkh^{-1} \in K$ for any $h \in H$. Now $hkh^{-1} = e$ and $hkh^{-1} = k$ both lead to a contradiction: the first implies $k = e$. If $hkh^{-1} = k$ for all $h \in H$, then $hk^2h^{-1} = (hkh^{-1})(hkh^{-1}) = k^2$, and it follows that H and K commute. Then by (c) $G' \cong H \times K$ and it follows that H is a normal subgroup, a contradiction with our assumption.

Problem 2. (a) For the first claim, show that if $a + N = b + N$ in R/N then $\phi(a) + N' = \phi(b) + N'$ to show the map is well-defined. The homomorphism property is a direct verification. Assume $\phi(R) = R'$. If $\phi(a) + \phi[N] = \phi[N]$, then $\phi(a) = \phi(n)$ for some $n \in N$. Then $a - n \in ker(\phi) \subseteq N$, so $a - n = n'$ for $n' \in N$. Then $a + N = N$, showing injectivity of ψ. Surjectivity follows from surjectivity of ϕ.

For (b), it is a theorem that R/M is a field for M a maximal ideal in a commutative ring with unity. Using the isomorphism ψ from (1), show that also $R'/\phi[M]$ is a field (note that $1' + \phi[M]$ is the unity in $R'/\phi[M]$ and show that every non-zero element has a multiplicative inverse). By the converse direction in the theorem, $\phi[M]$ is maximal in R'.

For (c), it is known that the maximal ideals in the ring $\mathbb{Z}$ are $p\mathbb{Z}$. For every prime p and $n \geq 1$, let $\phi : \mathbb{Z} \to \mathbb{Z}_{p^n}$ be the homomorphism given by $\phi(k)$ equals the remainder of the division of k by p^n. Then $\phi(1) = 1$ and $ker\phi = p^n\mathbb{Z} \subset p\mathbb{Z}$. By (b), $\phi[p\mathbb{Z}]$ is a maximal ideal in $\mathbb{Z}_{p^n}$. Note that $\phi[p\mathbb{Z}]$ is the ideal of $\mathbb{Z}_{p^n}$ generated by p.

Problem 3. (a) Let $\alpha = \sqrt{2} + i$. Then $\alpha^2 = 1 + 2i\sqrt{2}$, and by squaring again it follows that α is a zero of the polynomial $f(x) = x^4 - 2x^2 + 9$. Since none of the divisors of 9 is a zero, $f(x)$ has no linear terms. Suppose that $f(x)$ is reducible over $\mathbb{Q}$. Then $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ in $\mathbb{Q}[x]$. But $f(x) \in \mathbb{Z}[x]$, so it is enough to assume $a, b, c, d \in \mathbb{Z}$. We get that $x^3(c+a)+x^2(b+d+ac+2)+bd-9 = 0$. Solving $bd = 9$, $c+a = 0$ and $b+d+ac = -2$ in $\mathbb{Z}$ gives a contradiction. Hence our assumption was false, so $f(x)$ is irreducible over $\mathbb{Q}$.

The conjugates of α over $\mathbb{Q}$ are $\sqrt{2} - i$, $-\sqrt{2} + i$ and $-\sqrt{2} - i$. Thus $K = \mathbb{Q}(\sqrt{2}, i)$. Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (irreducible polynomial $x^2 - 2$) and $[K : [\mathbb{Q}(\sqrt{2})] = 2$ (irreducible polynomial is $x^2 + 1$ because $i \notin \mathbb{Q}(\sqrt{2})$), we have $[K : \mathbb{Q}] = 4$.

Let $G(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ where σ_1 is the identity automorphism of K. The other automorphisms are given by $\sigma_2(\alpha) = \sqrt{2} - i$, $\sigma_3(\alpha) = -\sqrt{2} + i$ and $\sigma_4(\alpha) = -\sqrt{2} - i$. On the basis elements, $\sigma_2(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(i) = -i$, $\sigma_3(\sqrt{2}) = -\sqrt{2}$ and $\sigma_3(i) = i$, and finally $\sigma_4(\sqrt{2}) = -\sqrt{2}$, $\sigma_4(i) = -i$. It follows that $\sigma_j^2 = \sigma_1$ for $j = 2, 3, 4$, so $G(K/\mathbb{Q})$ is isomorphic to the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$. By the Galois correspondence, the subgroups $\{\sigma_1, \sigma_2\}$, $\{\sigma_1, \sigma_3\}$ and $\{\sigma_1, \sigma_4\}$ correspond to the intermediate subfields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ and $\mathbb{Q}(i\sqrt{2})$.