Module MA3411, Michaelmas Term 2009 Relevant Examination Questions from the MA311 2008 Paper

David R. Wilkins

1. (a) *(3 marks) Let G be a group. What is meant by saying that a subset H of G is a* subgroup *of G? What is meant by saying that a subgroup N of G is a* normal subgroup *of G?*

   (b) *(2 marks) Let G and K be groups. What is meant by saying that a function $\theta: G \to K$ from G to K is a* homomorphism*? What is the* kernel *of a homomorphism $\theta: G \to K$?*

   (c) *(4 marks) Let G and K be groups, and let $\theta: G \to K$ be a homomorphism from G to K. Prove that the kernel of this homomorphism is a subgroup of G, and is a normal subgroup of G. Prove also that the homomorphism $\theta: G \to K$ is injective if and only if its kernel is the trivial subgroup $\{e_G\}$, where e_G denotes the identity element of G.*

   (d) *(4 marks) Let G_1 and G_2 be groups, let N_1 be a normal subgroup of G_1, and let N_2 be a normal subgroup of G_2. Prove that $N_1 \times N_2$ is a subgroup of $G_1 \times G_2$. Prove also that this subgroup is a normal subgroup of $G_1 \times G_2$.*

   (e) *(4 marks) Let G be a group, and let N_1 and N_2 be normal subgroups of G. Suppose that $N_1 \cap N_2 = \{e_G\}$, where e_G denotes the identity element of G. Prove that $xy = yx$ for all $x \in N_1$ and $y \in N_2$.*

   (f) *(3 marks) Let G be a finite group, and let N_1 and N_2 be normal subgroups of G. Suppose that $N_1 \cap N_2 = \{e_G\}$, and that $|G| = |N_1|\,|N_2|$. Prove that $G \cong N_1 \times N_2$.*

   (a) **Bookwork.**

   (b) **Bookwork.**

(c) **Bookwork.**

(d) Let e_1 and e_2 denote the identity elements of G_1, and G_2, and let (n_1, n_2) and (n_1', n_2') be elements of $N_1 \times N_2$. Then the identity element of $G_1 \times G_2$ is (e_1, e_2), and $(e_1, e_2) \in N_1 \times N_2$, since $e_1 \in N_1$ and $e_2 \in N_2$. Also $(n_1, n_2)(n_1', n_2') = (n_1 n_1',\, n_2 n_2') \in N_1 \times N_2$, since $n_1 n_1' \in N_1$ and $n_2 n_2' \in N_2$. Also $(n_1, n_2)^{-1} = (n_1^{-1}, n_2^{-1}) \in N_1 \times N_2$, since $n_1^{-1} \in N_1$ and $n_2^{-1} \in N_2$. Thus $N_1 \times N_2$ is a subgroup of G. Let (g_1, g_2) be an element of $G_1 \times G_2)$. Then

$$\begin{aligned} (g_1, g_2)(n_1, n_2)(g_1, g_2)^{-1} &= (g_1 n_1, g_2 n_2)(g_1^{-1}, g_2^{-1}) \\ &= (g_1 n_1 g_1^{-1}, g_2 n_2 g_2^{-1}) \in N_1 \times N_2. \end{aligned}$$

Thus $N_1 \times N_2$ is a normal subgroup of $G_1 \times G_2$.

(e) Let $x \in N_1$ and $y \in N_2$. Then $yx^{-1}y^{-1} \in N_1$ and $xyx^{-1} \in N_2$, since N_1 and N_2 are normal subgroups of G. But then $xyx^{-1}y^{-1} \in N_1 \cap N_2$, since $xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) = (xyx^{-1})y^{-1}$, and therefore $xyx^{-1}y^{-1} = e$. Thus $xy = yx$ for all $x \in N_1$ and $y \in N_2$.

(f) The function $\varphi\colon N_1 \times N_2 \to G$ which sends $(x, y) \in N_1 \times N_2$ to xy is a homomorphism. This homomorphism is injective, for if $xy = e$ for some $x \in N_1$ and $y \in N_2$, then $x = y^{-1}$, and hence $x \in N_1 \cap N_2$, from which it follows that $x = e$ and $y = e$. But $|N_1 \times N_2| = |N_1|\,|N_2| = |G|$, and any injective homomorphism between two finite groups of the same order is necessarily an isomorphism. Therefore the function $\varphi\colon N_1 \times N_2 \to G$ is an isomorphism, and thus $G \cong N_1 \times N_2$.

2. **Most of Question 2 on the 2008 MA311 paper did not cover MA3411 material**

3. *Throughout this question, let K be a field, and let $K[x]$ denote the ring of polynomials in a single indeterminate x with coefficients in the field K.*

   (a) *(5 marks) Let $f \in K[x]$ be a non-zero polynomial with coefficients in K. Prove that, given any polynomial $h \in K[x]$, there exist unique polynomials q and r in $K[x]$ such that $h = fq + r$ and either $r = 0$ or else $\deg r < \deg f$.*

   (b) *(5 marks) Let I be an ideal of the polynomial ring $K[x]$. Prove that there exists $f \in K[x]$ such that $I = (f)$, where (f) denotes the ideal of $K[x]$ generated by f.*

Polynomials $f_1, f_2, \ldots, f_k$ with coefficients in some field K are said to be coprime *if there is no non-constant polynomial that divides all of them.*

(c) *(5 marks) Let $f_1, f_2, \ldots, f_k$ be coprime polynomials with coefficients in the field K. Prove that there exist polynomials $g_1, g_2, \ldots, g_k$ with coefficients in K such that*

$$f_1(x)g_1(x) + f_2(x)g_2(x) + \cdots + f_k(x)g_k(x) = 1.$$

(d) *(5 marks) Let f, g and h be polynomials with coefficients in the field K. Suppose that both of the polynomials f and g divide h, and that the polynomials f and g are coprime. Prove that the product polynomial fg divides h.*

(a) **Bookwork.**

(b) **Bookwork.**

(c) **Bookwork.**

(d) It follows from (c) that there exist polynomials p and q with coefficients in K such that $1 = pf + qg$ (where 1 denotes the constant polynomial whose value is the identity element 1 of the field K). Then $h = pfh + qgh$. Now h is divisible by g, and therefore fh is divisible by fg. Also h is divisible by f, and therefore gh is divisble by fg. It follows that $pfh + qgh$ is divisible by fg, and thus h is divisible by fg, as required.

4. (a) *(3 marks) What is a* field extension*? What is meant by saying that a field extension is* finite*? What is the* degree $[L\colon K]$ *of a finite field extension $L\colon K$?*

(b) *(3 marks) Let $L\colon K$ be a field extension. What is meant by saying that an element α of L is* algebraic *over K? What is meant by saying that the field extension $L\colon K$ is* algebraic*?*

(c) *(10 marks) State and prove the Tower Law for field extensions.*

(d) *(4 marks) Prove that any finite field extension is algebraic.*

The above question is bookwork in its entirety.

5. (a) *(10 marks) State and prove the* Primitive Element Theorem*. [You may use without proof the result that the multiplicative group of non-zero elements of a finite field is cyclic.]*

(b) (6 marks) Prove that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

(c) (4 marks) What is the degree of the minimum polynomial of $\sqrt{3} + \sqrt{5}$ *over the field* $\mathbb{Q}$ *of rational numbers? [Briefly justify your answer. You may use, without proof, the fact that* $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$. *Note that you are* not *asked to find the minimum polynomial itself.]*

(a) **Bookwork.**

(b) $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$. But $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ is by definition the smallest subfield of the field of complex number that contains $\sqrt{3} + \sqrt{5}$, and is contained in every other such subfield. Therefore $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \subset \mathbb{R}(\sqrt{3}, \sqrt{5})$.

Let $\alpha = \sqrt{3} + \sqrt{5}$. Then $\alpha^2 = 8 + 2\sqrt{15}$ and $\alpha^3 = 18\sqrt{3} + 14\sqrt{5}$. Therefore $\sqrt{3} = \frac{1}{4}(\alpha^3 - \alpha)$. It follows that $\sqrt{3} \in \mathbb{Q}(\alpha)$. But then $\sqrt{5} \in \mathbb{Q}(\alpha)$, as $\sqrt{5} = \alpha - \sqrt{3}$. It follows that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbb{Q}(\sqrt{3} + \sqrt{5})$. We conclude that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{R}(\sqrt{3}, \sqrt{5})$, as required.

(c) The minimum polynomial of $\sqrt{3} + \sqrt{5}$ of $\mathbb{Q}$ is of degree 4. Indeed $\sqrt{5}$ is a root of the polynomial $x^2 - 5$, and the coefficients of this polynomial belong to $\mathbb{Q}$, and therefore belong to $\mathbb{Q}(\sqrt{3})$. Therefore the minimum polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{3})$ must divide $x^2 - 5$. But this minimum polynomial is not of degree 1, since $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$. Therefore $x^2 - 5$ is the minimum polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{3})$, and thus $[\mathbb{Q}(\sqrt{3}, \sqrt{5})\colon \mathbb{Q}(\sqrt{3})] = 2$. Also $x^2 - 3$ is the minumum polynomial of $\sqrt{3}$ over $\mathbb{Q}$, and therefore $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$. It follows from the Tower Law and (b) that

$$\begin{aligned} [\mathbb{Q}(\sqrt{3} + \sqrt{5})\colon \mathbb{Q}] &= [\mathbb{Q}(\sqrt{3}, \sqrt{5})\colon \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{3}, \sqrt{5})\colon \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 4. \end{aligned}$$

But the degree of this field extension is equal to the degree of the minimum polynomial of $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$. The result follows.

6. *(a) (3 marks) Let* $L\colon K$ *be a field extension, and let* f *be a polynomial with coefficients in* K. *What is meant by saying that the polynomial* f splits *over* L? *What is meant by saying that* L *is a* splitting field *for* f *over* K?

(b) (10 marks) Let K_1 *and* K_2 *be fields, let* $\sigma\colon K_1 \to K_2$ *be an isomorphism from* K_1 *to* K_2, *let* f *be a polynomial with coefficients*

in K_1, let $\sigma_*(f)$ be the polynomial with coefficients in K_2 that corresponds to f under σ, and let L_1 and L_2 be splitting fields for f and $\sigma_*(f)$ over K_1 and K_2 respectively. Prove that there exists an isomorphism $\tau\colon L_1 \to L_2$ which extends $\sigma\colon K_1 \to K_2$.

(c) *(2 marks) What is meant by saying that a field extension $L\colon K$ is* normal*?*

(d) *(5 marks) Determine which, if any, of the following field extensions are normal:—*

(i) $\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}$;

(ii) $\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}$;

(iii) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)\colon \mathbb{Q}$.

[Briefly justify your answers. You may use without proof the result that any splitting field extension is a normal extension. Here $i^2 = -1$, and $\sqrt[3]{2}$ denotes the unique positive real number ξ satisfying $\xi^3 = 2$.]

(a) **Bookwork.**

(b) **Bookwork.**

(c) **Bookwork.**

(d) The field extension $\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}$ is normal, since $\mathbb{Q}(\sqrt{2})$ is a splitting field for the polynomial $x^2 - 2$ over $\mathbb{Q}$.

The field extension $\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}$ is not normal. An application of Eisenstein's criterion shows that the polynomial $x^3 - 2$ is irreducible over the field $\mathbb{Q}$ of rational numbers. It has exactly one real root $\sqrt[3]{2}$. But $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of the field of real numbers. Therefore the irreducible polynomial $x^3 - 2$ has a root in the field $\mathbb{Q}(\sqrt[3]{2})$ but does not split over this field.

The field extension $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)\colon \mathbb{Q}$ is normal. Indeed let $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$, and let $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2} i$. Then $\omega \in L$, and

$$x^3 - 2 = (x - \xi)(x - \omega\xi)(x - \omega^2\xi),$$

where $\xi = \sqrt[3]{2}$. It follows from this that L is a splitting field for the polynomial $(x^3 - 2)(x^2 - 3)(x^2 + 1)$ over $\mathbb{Q}$, and therefore the extension $L\colon \mathbb{Q}$ is normal.

7. *Let K be a subfield of the field of complex numbers that contains the complex number ω, where $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2} i$. (Note that $\omega \neq 1$, $\omega^3 = 1$*

and $1+\omega+\omega^2=0$.) Let L be an extension field of K with $[L\colon K]=3$, and let f be a cubic polynomial with coefficients in K that splits over L but not over K. Let α, β and γ denote the roots of f in L and let

$$\lambda=\alpha+\omega\beta+\omega^2\gamma,\quad \mu=\alpha+\omega^2\beta+\omega\gamma.$$

(a) (10 marks) Show that there exists a K-automorphism θ of L such that $\theta(\alpha)=\beta$, $\theta(\beta)=\gamma$ and $\theta(\gamma)=\alpha$. What are $\theta(\lambda)$ and $\theta(\mu)$?

(b) (5 marks) Explain why $\lambda^3\in K$, $\mu^3\in K$ and $\lambda\mu\in K$.

(c) (5 marks) Find formulae expressing α, β and γ in terms of ω, λ, μ and c, where $c=\alpha+\beta+\gamma$.

(a) If the polynomial splits over some subfield M of L then $[M\colon K]>1$ and $[M\colon K]$ divides $[L\colon K]$, and therefore $[M\colon K]=3$ and $M=L$. It follows from this that the polynomial f cannot split over any proper subfield of L that contains K, and therefore L is a splitting field for the polynomial f over K. It follows from standard theorems that the field extension $L\colon K$ is finite, normal and separable, and therefore $|\Gamma(L\colon K)|=[L\colon K]=3$.

Any group of order 3 is a cyclic group. Any element of the Galois group is determined by the corresponding permutation of the roots of the polynomial f. A generator φ of the Galois group must induce a permutation of $\{\alpha,\beta,\gamma\}$ that is over order 3. Then either $\varphi(\alpha)=\beta$, $\varphi(\beta)=\gamma$ and $\varphi(\gamma)=\alpha$, in which case we can take $\theta=\varphi$, or else either $\varphi(\alpha)=\gamma$, $\varphi(\gamma)=\beta$ and $\varphi(\beta)=\alpha$, in which case we can take $\theta=\varphi^2$.

Now $\theta(\omega)=\omega$, since $\omega\in K$ and θ fixes all elements of the ground field K. It follows that

$$\begin{aligned}\theta(\lambda)&=\beta+\omega\gamma+\omega^2\alpha=\omega^2\lambda\\ \theta(\mu)&=\beta+\omega^2\gamma+\omega\alpha=\omega\mu\end{aligned}$$

(b) Now

$$\begin{aligned}\theta(\lambda^3)&=(\theta(\lambda))^3=(\omega^2\lambda)^3=\omega^6\lambda^3=\lambda^3,\\ \theta(\mu^3)&=(\theta(\mu))^3=(\omega\mu)^3=\omega^3\mu^3=\mu^3,\end{aligned}$$

and

$$\theta(\lambda\mu)=\theta(\lambda)\theta(\mu)=(\omega^2\lambda)(\omega\mu)=\omega^3\lambda\mu=\lambda\mu.$$

Also θ generates the Galois group $\Gamma(L\colon K)$. Therefore λ^3, μ^3 and $\lambda\mu$ belong to the fixed field of the Galois group $\Gamma(L\colon K)$. But this fixed field is the ground field K, because the extension $L\colon K$ is a splitting field extension, and thus a Galois extension. Therefore $\lambda^3 \in K$, $\mu^3 \in K$ and $\lambda\mu \in K$.

(c)

$$\begin{aligned} c+\lambda+\mu &= 3\alpha+(1+\omega+\omega^2)(\beta+\gamma)=3\alpha \\ c+\omega\lambda+\omega^2\mu &= 3\gamma+(1+\omega+\omega^2)(\alpha+\beta)=3\gamma \\ c+\omega^2\lambda+\omega\mu &= 3\beta+(1+\omega+\omega^2)(\alpha+\gamma)=3\beta \end{aligned}$$

Thus

$$\alpha=\frac{1}{3}(c+\lambda+\mu), \beta=\frac{1}{3}(c+\omega^2\lambda+\omega\mu), \gamma=\frac{1}{3}(c+\omega\lambda+\omega^2\mu).$$