# Modules MA3411/MA3412, Hilary Term 2010 Relevant Examination Questions from the MA311 2006 Paper

David R. Wilkins

1. *(a) Let $S$ be a subgroup of the group $\mathbb{Z}$ of integers (where the group operation is addition of integers). Prove that there exists some non-negative integer $m$ such that $S = m\mathbb{Z}$ (where $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$).*

   *(b) Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. Prove that there exist integers*
   *$u_1, u_2, \ldots, u_r$ such that*

   $$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r,$$

   *where $(a_1, a_2, \ldots, a_r)$ denotes the greatest common divisor of*

   $$a_1, a_2, \ldots, a_r.$$

   *(c) Let $x$ and $m$ be integers that are coprime. Prove that there exists some integer $y$ such that $xy \equiv 1$ (mod $m$).*

   *(d) Let $p$ be a prime number. Prove the theorem, due to Fermat, which states that $x^p \equiv x$ (mod $p$) for all integers $x$.*

   **The question above is a bookwork question set on material not formally included as such in the MA3411 and MA3412 syllabus. Nevertheless, parts (a) and (b) have some relevance with regard to the basic foundational material, and analogous results, concerning polynomial rings, and concerning principal ideal domains in general are to be found in the MA3411/MA3412 course material in 2009/10.**

2. *(a) Let $p$ be a prime number, and let $x$ be an integer coprime to $p$. What is meant by saying that $x$ is a* quadratic residue *of $p$?*

*(b) Which of the integers between 1 and 12 are quadratic residues of 13, and which are quadratic non-residues of 13?*

*(c) State the* Quadratic Reciprocity Law, *and prove its validity.*

*[You may use, without proof, the lemma due to Gauss, which states that, if $p$ is an odd prime number, if $m = (p-1)/2$, and if $x$ is an integer coprime to $p$ then the Legendre symbol $\left(\dfrac{x}{p}\right)$ has the value $(-1)^r$, where $r$ is the number of pairs $(j, u)$ of integers satisfying $1 \leq j \leq m$ and $1 \leq u \leq m$ for which $xj \equiv -u \pmod{p}$.]*

**The above question is a question on number theory not relevant to MA3411/MA3412 in 2009/10. All parts other than (c) are bookwork.**

3. *(a) Let $H$ be a subgroup of the group $\mathbb{Z}^n$, where $n$ is some positive integer, the elements of $\mathbb{Z}^n$ are ordered $n$-tuples of integers, and the group operation on $\mathbb{Z}^n$ is (vector) addition. What is meant by saying that a list $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_r$ of elements of $\mathbb{Z}^n$ is an* integral basis *of the subgroup $H$?*

*(b) A basic theorem concerning subgroups of $\mathbb{Z}^n$ (where $n$ is some positive integer) states that, given any non-trivial subgroup $H$ of $\mathbb{Z}^n$, there exists an integral basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of $\mathbb{Z}^n$, a positive integer $s$, where $s \leq n$, and positive integers $k_1, k_2, \ldots, k_s$ for which $k_1\mathbf{b}_1, k_2\mathbf{b}_2, \ldots, k_s\mathbf{b}_s$ is an integral basis of $H$. Using this theorem, or otherwise, prove that any finitely-generated Abelian group is isomorphic to a direct product of cyclic groups.*

*(c) Write down a list of Abelian groups of order 9 with the property that every Abelian group of order 9 is isomorphic to exactly one of the groups in this list. [Fully justify your answer.]*

*(c) Prove that any Abelian group of order 14 is cyclic.*

**This question concerns material not included in MA3411 and MA3412 in 2010. Parts (a) and (b) are bookwork linked to the 311 course material in 2005/6.**

4. *(a) Let $G$ be a finite group, and let $p$ be a prime number that divides the order of $G$. What is a* Sylow $p$-subgroup *of $G$?*

*(b) Prove the Second Sylow Theorem, which states that if $G$ is a finite group, and if $p$ is a prime number dividing the the order of $G$, then all all Sylow $p$-subgroups of $G$ are conjugate, and $p$-subgroup of $G$ is contained in some Sylow $p$-subgroup of $G$, and the number of*

*Sylow $p$-subgroups of $G$ divides the order $|G|$ of $G$ and is congruent to 1 modulo $p$.*

**Bookwork question not relevant to the MA3411/MA3412 syllabus.**

5. *(a) What is a* Noetherian ring*?*

   *(b) Prove* Hilbert's Basis Theorem*, which states that if $R$ is a Noetherian ring, then so is $R[x]$.*

6. *In this question, let $K$ be a field, let $K[X_1, X_2, \ldots, X_n]$ denote the ring of polynomials in independent indeterminates $X_1, X_2, \ldots, X_n$ with coefficients in $K$, and let $\mathbb{A}^n(K)$ denote $n$-dimensional affine space over the field $K$ which is defined to be the set $K^n$ of ordered $n$-tuples with components belonging to the field $K$.*

   *(a) What is an* algebraic set *in $\mathbb{A}^n(K)$?*

   *(b) Prove that the intersection of any collection of algebraic sets in $\mathbb{A}^n(K)$ is an algebraic set in $\mathbb{A}^n(K)$.*

   *(c) Prove that the union of two algebraic sets in $\mathbb{A}^n(K)$ is an algebraic set in $\mathbb{A}^n(K)$.*

   *(d) Give the definition of the* Zariski topology *on $\mathbb{A}^n(K)$.*

   *(e) Determine which of the following are algebraic sets in $\mathbb{A}^2(\mathbb{C})$:—*

   *(i) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) : z \neq 0$ and $w \neq 0\}$;*

   *(ii) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) : z \neq 0$ and $w = 1/z\}$;*

   *(iii) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) : |z|^2 + |w|^2 = 1\}$;*

   *(iv) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) : w = e^z\}$.*

   *[Briefly justify your answers.]*

   (a) **Bookwork.**

   (b) **Bookwork.**

   (c) **Bookwork.**

   (d) **Bookwork.**

   (e)

   (i) Not an algebraic set. Any complex line (i.e., one-dimensional affine subspace) should be contained in the set, or intersect the set in a finite number of points. That is not the case for the complex line $\{(z, w) \in \mathbb{C}^2 : w = 1\}$, whose intersection with the set contains all points of the line with the exception of the point $(0, 1)$.

(ii) This is the algebraic set $\{(z, w) \in \mathbb{C} : zw = 1\}$.

(iii) Not an algebraic set. The complex line $\{(z, w) \in \mathbb{C}^2 : w = 0\}$ intersects the set in the circle $w = 0$, $|z| = 1$, which is an infinite set, but is not the whole of the complex line.

(iv) Not an algebraic set. The complex line $\{(z, w) \in \mathbb{C}^2 : w = 1\}$ intersects the given set at points of the set $\{(2\pi in, 1) : n \in \mathbb{Z}\}$, which is an infinite set, but not the whole of the complex line.

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

*(b) State the Tower Law for field extensions.*

*(c) Let $K$ be a field, and let $\alpha$ be an element of some extension field of $K$. Suppose that $\alpha$ is algebraic over $K$. Prove that the simple field extension $K(\alpha)\colon K$ is finite, and also that the degree $K(\alpha)\colon K]$ of this simple field extension is equal to the degree of the minimum polynomial of $\alpha$ over $K$. [You may use without proof the result that the quotient ring $K[x]/(f)$ is a field, where $K[x]$ is the ring of polynomials in the indeterminate $x$ with coefficients in $K$, and where $(f)$ is the ideal of $K[x]$ generated by an irreducible polynomial $f$ with coefficients in $K$. You may also use without proof the existence and basic properties of the minimum polynomial of $\alpha$ over $K$.]*

*(d) Let $K$ be a field, and let $\alpha$ be an element of some extension field of $K$. Suppose that $\alpha$ is the root of some cubic polynomial with coefficients in $K$, and that this cubic polynomial is irreducible over $K$. Let $\beta$ be an element of $K(\alpha)$ with the property that $\beta^2 \in K$. Prove that $\beta \in K$.*

(a) **Bookwork.**

(b) **Bookwork.**

(c) **Bookwork.**

(d) $\beta$ is a root of the polynomial $x^2 - \beta^2$ whose coefficients lie in the field $K$. Therefore the degree of the minimum polynomial of $\beta$ over $K$ is at most 2. But $[K(\alpha)\colon K] = 3$ (by (c)), and

$$[K(\alpha)\colon K] = [K(\alpha)\colon K(\beta)][K(\beta)\colon K]$$

by the Tower Law. It follows that $[K(\beta)\colon K] = 1$ (since it is a divisor of 3 that is less than 3), and therefore $\beta \in K$.

8. *(a) What is meant by saying that a field extension is* normal*? What is meant by saying that a field extension is* separable*?*

   *(b) Give the definition of the* Galois group $\Gamma(L\colon K)$ *of a field extension* $L\colon K$.

   *(c) Let $L$ be a field, let $G$ be a finite group of automorphisms of $L$, and let $K$ be the fixed field of $G$ (i.e.,*

   $$K = \{a \in L : \sigma(a) = a \textit{ for all } \sigma \in G\}.)$$

   *Prove that each element $\alpha$ of $L$ is algebraic over $K$, and that the minimum polynomial of $\alpha$ over $K$ is the polynomial*

   $$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k),$$

   *where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are distinct and are the elements of the orbit of $\alpha$ under the action of $G$ on $L$.*

   *(d) Let $L$ be a field, let $G$ be a finite group of automorphisms of $L$, and let $K$ be the fixed field of $G$. Prove that the field extension $L\colon K$ is a Galois extension (i.e., an extension that is finite, normal and separable). Show moreover that $G$ is the Galois group $\Gamma(L\colon K)$ of $L\colon K$, and that $|G| = [L\colon K]$.*

   **The above question is bookwork in its entirety.**

9. *Let $L$ be the subfield of $\mathbb{C}$ which is a splitting field for the polynomial $f$ over the field $\mathbb{Q}$ of rational numbers, where*

   $$f(x) = \sum_{j=0}^{4} (x+1)^j = x^4 + 5x^3 + 10x^2 + 10x + 5.$$

   *(a) Show that the roots of the polynomial $f$ are of the form $\zeta^j - 1$ for $j = 1, 2, 3, 4$, where*

   $$\zeta = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5}).$$

   *(Here $i^2 = -1$.)*

   *(b) Is the polynomial $f$ irreducible over $\mathbb{Q}$? (Briefly justify your answer.)*

   *(c) Prove that the Galois group of the polynomial $f$ is a cyclic group of order 4, and, for each automorphism of $L$ belonging to the Galois group of $f$, and for each root of the polynomial $f$, find the image of the root under the automorphism.*

*(d) Let $M = \mathbb{Q}(\theta)$ where $\theta = \cos(2\pi/5)$. Explain why $M$ is the unique subfield of $L$ for which $\mathbb{Q} \subset M \subset L$, $M \neq \mathbb{Q}$ and $M \neq L$. Is $M\colon\mathbb{Q}$ a normal extension of $\mathbb{Q}$? [Justify your answer.]*

(a) A straightforward calculation shows that

$$xf(x) = ((x+1)-1)\sum_{j=0}^{r}(x+1)^j = (x+1)^5 - 1.$$

Thus if $\alpha$ is a root of $f$ then $\alpha + 1$ is a 5th root of unity, distinct from 1, and therefore $\alpha + 1 = \xi^j$ for some integer $j$ satisfying $0 < j < 5$.

(b) The polynomial $f$ is irreducible. This follows from an immediate application of Eisenstein's criterion for irreducibility, with the prime equal to 5, given that 5 divides all coefficients with the exception of the leading coefficient, and 25 does not divide the constant coefficient.

(c) The Galois group of the polynomial can be regarded as the Galois group $\Gamma(L\colon\mathbb{Q})$ of the field extension $L\colon\mathbb{Q}$, where $L = \mathbb{Q}(\zeta)$, since $\mathbb{Q}(\zeta)$ is a splitting field for $f$ over $\mathbb{Q}$. Let $\varphi$ be a $\mathbb{Q}$-automorphism of $L$. Then $\varphi(\zeta)^5 = \varphi(\zeta^5) = 1$ and $\varphi(\zeta) \neq 1$, and therefore $\varphi(\zeta) = \zeta^r$ for some integer $r$ satisfying $0 < r < 5$.

Let $\alpha_j = \zeta^j - 1$ for each integer $j$. Then the roots of $f$ are $\alpha_1$, $\alpha_2$, $\alpha_3$ and $\alpha_4$. Also $\alpha_j = \alpha_k$ if and only if $j \equiv k \pmod 5$. Now if $\varphi \in \Gamma(L\colon\mathbb{Q})$ satisfies $\varphi(\zeta) = \zeta^r$ then $\varphi(\zeta^j) = \zeta^{rj}$, and therefore $\varphi(\alpha_j) = \alpha_{rj}$ for all integers $j$.

Now the polynomial $f$ is irreducible, and therefore the Galois group acts transitively on its roots. It follows that the automorphism $\varphi$ may be chosen such that $\varphi(\alpha_1) = \alpha_2$. Then $\varphi(\alpha_2) = \alpha_4$, $\varphi(\alpha_4) = \alpha_8 = \alpha_3$, $\varphi(\alpha_3) = \alpha_6 = \alpha_1$. Therefore $\varphi$ is an automorphism of order 4. But $f$ is the minimum polynomial

$$|\Gamma(L\colon\mathbb{Q})| = [L\colon\mathbb{Q}] = [\mathbb{Q}(\alpha_1)\colon\mathbb{Q}] = \deg f = 4.$$

It follows that the Galois group $\Gamma(L\colon\mathbb{Q})$ is a cyclic group of order 4, generated by $\varphi$. Its elements are $\iota, \varphi, \varphi^2, \varphi^3$, where $\iota$ denotes the identity automorphism. Moreover

$$\varphi(\alpha_1) = \alpha_2, \quad \varphi(\alpha_2) = \alpha_4, \quad \varphi(\alpha_4) = \alpha_3, \quad \varphi(\alpha_3) = \alpha_1,$$

$$\varphi^2(\alpha_1) = \alpha_4, \quad \varphi^2(\alpha_4) = \alpha_1, \quad \varphi^2(\alpha_2) = \alpha_3, \quad \varphi^2(\alpha_3) = \alpha_2,$$

$$\varphi^3(\alpha_1) = \alpha_3, \quad \varphi^3(\alpha_3) = \alpha_4, \quad \varphi^3(\alpha_4) = \alpha_2, \quad \varphi^3(\alpha_2) = \alpha_1.$$

(d) The field extension $L\colon\mathbb{Q}$ is a Galois extension, being finite, normal and separable, and therefore Galois Theory ensures that there is a one-to-one correspondence between fields $M$ satisfying $\mathbb{Q} \subset M \subset L$ and subgroups of the Galois group. If $M \neq \mathbb{Q}$ and $M \neq L$ then $[M\colon\mathbb{Q}] = 2$, and therefore $\Gamma(L\colon M)$ must be a subgroup of $\Gamma(L\colon\mathbb{Q})$ whose order and index are equal to 2. There is only one such subgroup, and it is the cyclic subgroup generated by $\varphi^2$. We deduce that there can only exist one such field $M$ satisfying the given conditions. Moreover it follows from standard properties of the Galois correspondence that this field $M$ is the fixed field of the automorphism $\varphi^2$. But on examining the action of $\varphi^2$ on the roots of $f$, we see that $\varphi$ is the restriction to $L$ of the automorphism of $\mathbb{C}$ defined by complex conjugation. Therefore $M = L \cap \mathbb{R}$.

Now $\zeta, \zeta^2, \zeta^3, \zeta^4$ is a basis for $L$ as a vector space over $\mathbb{Q}$, and moreover any element of the fixed field $M$ of $\varphi^2$ must be a linear combination of $\zeta + \zeta^4$ and $\zeta^2 + \zeta^3$ with coefficients in $\mathbb{Q}$. Moreover $\zeta + \zeta^4 = 2\theta$ and $\zeta^2 + \zeta^3 = 4\theta^2 - 2$. It follows that $M = \mathbb{Q}(\theta)$, as required. $M$ is a normal extension of $\mathbb{Q}$ because its Galois group is a normal subgroup of the Abelian group $\Gamma(L\colon\mathbb{Q})$.