Modules MA3411/MA3412, Hilary Term 2010 Relevant Examination Questions from the MA311 2002 Paper

David R. Wilkins

1. *(a) Let x, y and m be integers with $m \neq 0$. Suppose that m divides xy and that m and x are coprime. Prove that m divides y.*

   (b) Let $m_1, m_2, \ldots, m_r$ be non-zero integers that are pairwise coprime. Let x be an integer that is divisible by m_i for $i = 1, 2, \ldots, r$. Prove that x is divisible by the product $m_1 \cdot m_2 \cdots m_r$ of $m_1, m_2, \ldots, m_r$.

   (c) State and prove the Chinese Remainder Theorem*.*

   (d) Find an integer x such that $x \equiv 2$ (mod 3) $x \equiv 3$ (mod 5) and $x \equiv 1$ (mod 7).

   Question on Number Theory, which is not included in the syllabus for MA3411 and MA3412.

2. *(a) Let m be a positive integer. What is meant by saying that some positive integer g is a* primitive root *modulo m?*

   (b) Let p be a prime number, and let x and y be integers coprime to p. Suppose that the congruence classes of x and y modulo p have the same order. Prove that there exists a non-negative integer k, coprime to the order of the congruence classes of x and y, such that $y \equiv x^k$ (mod p). [You may use without proof the fact that if f is any polynomial of order n with integer coefficients, and if p is any prime number, then the congruence $f(x) \equiv 0$ (mod p) has at most n integer solutions x in the range $0 \leq x < p$.]

   (c) Let p be a prime number. Prove that there exists a primitive root modulo p. [You may use without proof any standard properties of the Euler totient function ϕ, where, for any positive integer n,

$\phi(n)$ denotes the number of integers satisfying $0 \leq x < n$ that are coprime to n.]

Question on Number Theory, which is not included in the syllabus for MA3411 and MA3412.

3. *(a) What is meant by saying that a subgroup N of a group G is a* normal subgroup *of G? What is a* homomorphism *from a group G to a group K? What is the* kernel $\ker\theta$ *of a homomorphism $\theta\colon G \to K$?*

   (b) Let N be a normal subgroup of a group G. Prove that $xN = Nx$ for all $x \in G$.

   (c) Prove that if $\theta\colon G \to K$ is a homomorphism from a group G to a group K then the kernel $\ker\theta$ of θ is a normal subgroup of G.

   (d) Let G and K be groups, let $\theta\colon G \to K$ be a homomorphism from G to K. Let M_1 and M_2 be subgroups of K with $M_1 \subset M_2$, and let

$$N_1 = \{g \in G : \theta(g) \in M_1\}, \quad N_2 = \{g \in G : \theta(g) \in M_2\}.$$

   Suppose that M_1 is a normal subgroup of M_2. Prove that N_1 is a subgroup of G, and is a normal subgroup of N_2.

Note that it has been announced that no questions will be set in 2010 that deal directly with the material of Sections 1 and 2 of the lecture notes for MA3411. This is an example of such a question.

(a) **Bookwork.**

(b) **Bookwork.**

(c) **Bookwork.**

(d) Let $x \in N_1$. Then $\theta(x) \in M_1$, hence $\theta(x)^{-1} \in M_1$. But $\theta(x)^{-1} = \theta(x^{-1})$, since

$$\theta(x)\theta(x^{-1}) = \theta(xx^{-1}) = \theta(e_G) = e_K$$

and

$$\theta(x^{-1})\theta(x) = \theta(x^{-1}x) = \theta(e_G) = e_K,$$

Thus $\theta(x^{-1}) \in M_1$, and therefore $x^{-1} \in N_1$.

Let $x \in N_1$ and $y \in N_1$. Then $\theta(xy) = \theta(x)\theta(y)$, and $\theta(x)\theta(y) \in M_1$, and therefore $xy \in N_1$.

We have thus shown that $e_G \in N_1$, and that $x^{-1} \in N_1$ and $xy \in N_1$ for all $x \in N_1$ and $y \in N_1$. We deduce that N_1 is a subgroup of G.

Let $x \in N_1$ and $n \in N_2$. Then

$$\theta(nxn^{-1}) = \theta(n)\theta(x)\theta(n^{-1}) = \theta(n)\theta(x)\theta(n)^{-1}$$

and $\theta(n)\theta(x)\theta(n)^{-1} \in M_1$, since $\theta(x) \in M_1$, $\theta(n) \in M_2$, and M_1 is a normal subgroup of M_2. Therefore $nxx^{-1} \in N_1$. This proves that N_1 is a normal subgroup of N_2.

4. (a) *Let H be a non-trivial subgroup of $\mathbb{Z}^n$ (where the group operation on $\mathbb{Z}^n$ is the standard one of addition of n-tuples). What is meant by saying that elements $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_r$ of H constitute an* integral basis *of the subgroup H?*

   (b) *Let H be a non-trivial subgroup of $\mathbb{Z}^n$. Prove that 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.*

Bookwork question on material that is not included on the syllabus for MA3411/MA3412.

5. (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) *State and prove the Second Sylow Theorem.*

Bookwork question on material that is not included on the syllabus for MA3411/MA3412.

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

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

   (c) *Let $L\colon K$ be a finite field extension with $[L\colon K] = 77$. Explain briefly why there cannot exist any element of L whose minimal polynomial over K is a cubic polynomial.*

(a) **Bookwork.**

(b) **Bookwork.**

(c) Suppose that there were to exist an element α of L whose minimum polynomial over K was a cubic polynomial. Then $[K(\alpha)\colon K] = 3$, since the degree of this simple extension is equal to the degree of the minimum polynomial of α. But this is impossible since

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

by the Tower Law, and 3 does not divide 77.

7. *(a) 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) What is meant by saying that a field extension $L\colon K$ is normal*?*

   (c) Let $L\colon K$ be a field extension, where L is a splitting field over K for some polynomial with coefficients in K. Prove that the extension $L\colon K$ is normal.

   [You may use, without proof, the following theorem: 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. Then there exists an isomorphism $\tau\colon L_1 \to L_2$ which extends $\sigma\colon K_1 \to K_2$.]

   This question is bookwork in its entirety.

8. *(a) Let f be a polynomial with coefficients in a field K. Give the definition of the* Galois group *of the polynomial f over the field K.*

   (b) Prove that the Galois group of the polynomial $x^3 + 9x - 3$ over the field $\mathbb{Q}$ of rational numbers is isomorphic to the symmetric group Σ_3 of permutations of three objects.

   (a) **Bookwork.**

   (b) **Based on bookwork.** First we note that the polynomial $x^3 + 9x - 3$ is irreducible over the field $\mathbb{Q}$ of rational numbers. This follows directly on applying Eisenstein's criterion with the prime number equal to 3.

   Next we note that this polynomial has only one real root. Indeed the first derivative is $3x^2+9$ which has no real roots, and is strictly positive for all real x. The existence of one real root follows by Rolle's Theorem, or indeed by elementary calculus.

Let α be the real root of the polynomial, and let β and γ be the two non-real roots. Then $\overline{\beta} = \gamma$ (where $\overline{\beta}$ denotes the complex conjugate of β).

Let L be the splitting field for the polynomial over $\mathbb{Q}$ that is contained within the field of complex numbers. Then $L = \mathbb{Q}(\alpha, \beta, \gamma)$. The restriction $\tau\colon L \to L$ of complex conjugation to the field L is a $\mathbb{Q}$-automorphism of L, and thus represents an element τ of the Galois group $\Gamma(L\colon \mathbb{Q})$. Clearly $\tau^2 = \iota$, where ι denotes the identity automorphism of L. It follows from Lagrange's Theorem that $|\Gamma(L\colon \mathbb{Q})|$ is divisible by 2.

Also $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 3$, since the polynomial $x^3 + 9x + 3$, being irreducible and monic, is the minimum polynomial over α over $\mathbb{Q}$, and the degree of such a simple extension is equal to the degree of the minimum polynomial of α over $\mathbb{Q}$.

It follows that $[L\colon \mathbb{Q}]$ is divisible by 3, since

$$[L\colon \mathbb{Q}] = [L\colon \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha)\colon \mathbb{Q}]$$

by the Tower Law. But $[L\colon \mathbb{Q}] = |\Gamma(L\colon \mathbb{Q})|$, since $L\colon \mathbb{Q}$ is a Galois extension.

We see therefore that the order $|\Gamma(L\colon \mathbb{Q})|$ of the Galois group is divisible by 2 and by 3, and is therefore divisible by 6.

But any $\mathbb{Q}$-automorphism of L is determined by its action on the roots α, β and γ of the polynomial f, and induces a permutation of those roots. The Galois group $\Gamma(L\colon \mathbb{Q})$ is therefore isomorphic to a subgroup of the group of permutations of three objects, those three objects being the three roots of the polynomial. This permutation group is of order 6. Therefore the Galois group is isomorphic to the permutation group itself, as required.

9. *Let p be a prime number, and let K be a field of characteristic zero with the property that the polynomial $x^p - 1$ splits over K.*

   (a) *Let $L\colon K$ be a Galois extension of K with $[L\colon K] = p$. Prove that there exists an element α of L such that $L = K(\alpha)$ and $\alpha^p \in K$.*

   *[*Hint*: consider the action of a generator σ of the Galois group $\Gamma(L\colon K)$ on the elements α_j given by*

$$\alpha_j = \beta + \omega^j \sigma(\beta) + \omega^{2j} \sigma^2(\beta) + \cdots + \omega^{(p-1)j} \sigma^{p-1}(\beta),$$

   where $\beta \in L \setminus K$ and ω is a primitive pth root of unity belonging to K.]

(b) Let $c \in K$. Prove that if the polynomial $x^p - c$ has no root in K then its Galois group over K is a cyclic group of order p.

(a) **Bookwork.**

(b) **Based on bookwork.** Let L be a splitting field for the polynomial $x^p - c$ over K, and let α be a root of that polynomial in L. The field K contains a primitive pth root of unity ω, since $x^p - 1$ splits over K. Then the roots of $x^p - c$ are of the form $\alpha\omega^j$ for $0 \leq j < p$. These roots all belong to $K(\alpha)$, and therefore $L = K(\alpha)$. It follows that $[L\colon K] \leq p$, since $[L\colon K]$ must be equal to the degree of the minimum polynomial of α over K. Let $\sigma \in \Gamma(L\colon K)$ be a non-trivial K-automorphism of L. Then $\sigma(\alpha) = \alpha\omega^r$ for some positive integer r coprime to p. But then $\sigma^j(\alpha) = \alpha\omega^{jr}$ for all integers j. It follows that $\sigma^j(\alpha) = \alpha$ if and only if jr is divisible by p, and thus $\sigma^j(\alpha) = \alpha$ if and only if j is divisible by p (since r is coprime to p). Thus the automorphism σ is of order p, and therefore $|\Gamma(L\colon K)| = [L\colon K] = p$. The result now follows from the fact that any cyclic group of prime order is cyclic.