Final exam in MAT2200, Spring 2018 - Solutions

Problem 1.

1a

Find all abelian groups, up to isomorphism, of order 27 and exponent 3. Can you do this without using the classification of finite abelian groups? Find all abelian groups of order 81. Justify your answer.

Solution: By the classification of finite abelian groups any abelian group of order 3^n is isomorphic to $\mathbb{Z}_{3^{a_1}} \times \cdots \times \mathbb{Z}_{3^{a_m}}$ for uniquely defined numbers $1 \leq a_1 \leq \cdots \leq a_m$ such that $a_1 + \cdots + a_m = n$. It follows that the abelian groups of order 27, up to isomorphism, are

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_3 \times \mathbb{Z}_9, \quad \mathbb{Z}_{27}.$$

Among these only $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ has exponent 3. This could also be proved by observing that any finite abelian group of exponent 3 is a vector space over the field $\mathbb{Z}_3$, hence it is isomorphic to $\mathbb{Z}_3^n$ for some n. To get a group of order 27 we must have $n = 3$.

In a similar way, the abelian groups of order 81, up to isomorphism, are

$$\mathbb{Z}_3^4, \quad \mathbb{Z}_3^2 \times \mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_{27}, \quad \mathbb{Z}_9 \times \mathbb{Z}_9, \quad \mathbb{Z}_{81}.$$

1b

Show that

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_3 \right\} \subset \mathrm{GL}_3(\mathbb{Z}_3)$$

is a nonabelian group of order 27 and exponent 3.

Solution: It is clear that H has 27 elements. We have

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & ac'+b+b' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}.$$

From this we see that H is closed under multiplication and since the inverse of

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{is} \quad \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix},$$

it is also closed under taking inverses. Hence H is a subgroup of $\mathrm{GL}_3(\mathbb{Z}_3)$. We also see that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3a & 3ac+3b \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

hence H has exponent 3. Finally, H is nonabelian, since, for example,

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Problem 2.

Let G be a group of order 2018.

2a

Show that G contains a normal cyclic subgroup H of order 1009. (You may use without checking that 1009 is a prime number.)

Solution: Since 1009 is a prime number dividing the order of G, by Cauchy's theorem there exists an element $a \in G$ of order 1009. Then $H = \langle a \rangle$ is a subgroup of G of index 2, hence it is normal. Alternatively, this can be deduced from Sylow's theorems.

2b

Show that G is either cyclic or isomorphic to the dihedral group of order 2018. (Recall that the latter group is generated by two elements a and b such that $a^{1009} = e$, $b^2 = e$ and $bab^{-1} = a^{-1}$.) Hint: if $b \in G$ is an element of order 2, then the formula $\alpha(h) = bhb^{-1}$ defines an automorphism α of $H \cong \mathbb{Z}_{1009}$ satisfying $\alpha^2 = \mathrm{id}$.

Solution: This was basically given in the assignment and can be solved from scratch as follows.

Let $a \in H$ be a generator. Since 2 divides the order of G, there is an element $b \in G$ of order 2. Then, following the hint, we get an automorphism α of $H \cong \mathbb{Z}_{1009}$ defined by $\alpha(h) = bhb^{-1}$. We have $\alpha^2 = \mathrm{id}$, hence if $\alpha(a) = a^k$, then $\alpha^2(a) = a^{k^2}$, and therefore $k^2 = 1$ in the ring $\mathbb{Z}_{1009}$. Since $\mathbb{Z}_{1009}$ is a field, the equation $x^2 - 1 = 0$ has only two solutions in $\mathbb{Z}_{1009}$: 1 and -1. Therefore either $bab^{-1} = a$ or $bab^{-1} = a^{-1}$.

In the first case we have a surjective (since $G = H \cup Hb$) homomorphism

$$\mathbb{Z}_{1009} \times \mathbb{Z}_2 \to G, \quad (1,0) \mapsto a, \quad (0,1) \mapsto b,$$

which must be injective as the orders of $\mathbb{Z}_{1009} \times \mathbb{Z}_2$ and G are the same. Thus in this case we have $G \cong \mathbb{Z}_{1009} \times \mathbb{Z}_2 \cong \mathbb{Z}_{2018}$.

In the second case we similarly have a surjective homomorphism $D_{2018} \to G$ mapping the standard generators of the dihedral group into a and b, respectively. Hence $D_{2018} \cong G$, since again both groups have the same orders.

Problem 3.

Let K be a field of characteristic different from 2, $\bar{K}$ be an algebraic closure of K, and $\alpha \in \bar{K} \setminus K$. Let f and g be the irreducible polynomials of α and α^2 over K.

3a

Assume $f(x) \in K[x^2]$, that is, $f(x) = h(x^2)$ for some polynomial $h \in K[x]$. Show that h is irreducible and conclude that $h = g$ and $[K(\alpha) : K(\alpha^2)] = 2$.

Solution: If h is not irreducible, say, $h = pq$ for some nonconstant polynomials p and q, then $f(x) = p(x^2)q(x^2)$ is not irreducible either, which is a contradiction. Since $h(\alpha^2) = f(\alpha) = 0$, we conclude that h is the irreducible polynomial of α^2, so $h = g$. Then

$$[K(\alpha) : K] = \deg f \quad \text{and} \quad [K(\alpha^2) : K] = \deg g = \frac{\deg f}{2},$$

hence $[K(\alpha) : K(\alpha^2)] = 2$.

3b

Assume now that $f(x) \notin K[x^2]$, so that f contains at least one nonzero term with an odd power of x. Show that $g(x^2)$ is divisible by $f(x)$ and $f(-x)$ and conclude that $K(\alpha) = K(\alpha^2)$.

Solution: Since $x = \alpha$ is a root of $g(x^2)$, the polynomial $g(x^2)$ must be divisible by $f(x)$. Similarly, $g(x^2)$ must be divisible by the irreducible polynomial of $-\alpha$ over K, which up to a scalar factor coincides with $f(-x)$. The irreducible polynomials $f(x)$ and $f(-x)$ cannot differ only by a scalar factor, since f contains nonzero odd degree terms (by assumption) and even degree terms (for example, the constant term). Hence $g(x^2)$ must be divisible by $f(x)f(-x)$, so $\deg g \geq \deg f$. Since we always have

$$\deg f = [K(\alpha) : K] \geq [K(\alpha^2) : K] = \deg g,$$

we conclude that $\deg f = \deg g$ and $K(\alpha^2) = K(\alpha)$.

As a byproduct we see that $g(x^2)$ coincides with $f(x)f(-x)$ up to a scalar factor, and by looking at the leading terms we conclude that $g(x^2) = (-1)^{\deg f} f(x)f(-x)$.

3c

Take $K = \mathbb{Q}$ and give examples of α, with $\alpha^2 \notin \mathbb{Q}$, illustrating 3a and 3b. In both cases write down the corresponding polynomials $f(x)$ and $g(x)$ and explain why f is irreducible.

Solution: For 3a take $\alpha = \sqrt[4]{2}$. Then $f(x) = x^4 - 2$ and $g(x) = x^2 - 2$. For 3b take $\alpha = \sqrt[3]{2}$. Then $f(x) = x^3 - 2$ and $g(x) = x^3 - 4$. In both cases f is irreducible by Eisenstein's criterion with $p = 2$.

Problem 4.

Let p be a prime number and $K \subset \mathbb{C}$ be the splitting field of the polynomial $f(x) = x^p - 2 \in \mathbb{Q}[x]$.

4a

Prove that for every natural number $n \geq 2$ we have $[\mathbb{Q}(2^{1/n}) : \mathbb{Q}] = n$.

Solution: The polynomial $x^n - 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion with prime number 2. Hence by adjoining any root of this polynomial we get an extension of degree n.

4b

Consider the pth primitive root of unity $\zeta_p = e^{2\pi i/p}$. Show that $K = \mathbb{Q}(2^{1/p}, \zeta_p)$ and conclude that $[K : \mathbb{Q}] = p(p-1)$. (You may use without explanation that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.)

Solution: The roots of f are $\zeta_p^k \, 2^{1/p}$, $k = 0, \ldots, p-1$. From this we see that K must contain both ζ_p and $2^{1/p}$, and then $K = \mathbb{Q}(2^{1/p}, \zeta_p)$, as $\zeta_p^k \, 2^{1/p} \in \mathbb{Q}(2^{1/p}, \zeta_p)$. The degree $[K\colon \mathbb{Q}]$ is divisible both by $[\mathbb{Q}(2^{1/p}) : \mathbb{Q}] = p$ and by $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, hence it is divisible by $p(p-1)$. On the other hand,

$$[K\colon \mathbb{Q}] = [\mathbb{Q}(2^{1/p}, \zeta_p) : \mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p) : \mathbb{Q}] \leq [\mathbb{Q}(2^{1/p}) : \mathbb{Q}][\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p(p-1).$$

Hence $[K : \mathbb{Q}] = p(p-1)$.

4c

Describe all elements of the Galois group $G(K/\mathbb{Q})$ by their actions on $2^{1/p}$ and ζ_p. Show next that $G(K/\mathbb{Q})$ is isomorphic to the group

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p \right\} \subset \mathrm{GL}_2(\mathbb{Z}_p),$$

called the $ax + b$ group *over the field $\mathbb{Z}_p$.*

Solution: Since every element of the Galois group maps every root of a polynomial in $\mathbb{Q}[x]$ into a root of the same polynomial, by taking the polynomials $x^p - 1$ (or $x^{p-1} + x^{p-2} + \cdots + 1$) and $x^p - 2$, we see that any $\sigma \in G(K/\mathbb{Q})$ satisfies

$$\sigma(\zeta_p) = \zeta_p^a \quad \text{and} \quad \sigma(2^{1/p}) = \zeta_p^b \, 2^{1/p}$$

for some $1 \leq a \leq p-1$ and $0 \leq b \leq p-1$. This gives us $p(p-1)$ possibilities. Since $G(K/\mathbb{Q})$ has order $[K : \mathbb{Q}] = p(p-1)$, all these possibilities are realized.

Denote by $\sigma_{a,b} \in G(K/\mathbb{Q})$ the element σ given by the above formulas. Then we can define a bijection from $G(K/\mathbb{Q})$ onto the $ax + b$ group by mapping $\sigma_{a,b}$ into the matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. It remains to check that this map is a group homomorphism. We have

$$(\sigma_{a,b} \circ \sigma_{c,d})(\zeta_p) = \sigma_{a,b}(\zeta_p)^c = \zeta_p^{ac}, \quad (\sigma_{a,b} \circ \sigma_{c,d})(2^{1/p}) = \sigma_{a,b}(\zeta_p)^d \sigma_{a,b}(2^{1/p}) = \zeta_p^{ad+b} 2^{1/p}.$$

This shows that $\sigma_{a,b} \circ \sigma_{c,d} = \sigma_{r,s}$, with $r \equiv ac \pmod p$ and $s \equiv ad + b \pmod p$. Since

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix},$$

this is what we need.