HOME EXAM
MAT2200

University of Oslo

Department of Mathematics

Problem 1 a) We are given the permutation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 4 & 7 & 8 & 5 & 1 & 6 & 2 & 9 \end{pmatrix}$$

We are asked to write σ as a product of disjoint cycles and to determine if σ is an even or odd permutation.
As disjoint cycles product we get:

$$(1347)(2109)(586)$$

Because we have odd number of transpositions we consider this an odd permutation.

Problem 1 b) The assignment requires us to show that the eight matrices given as

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

And we must show that the group is isomorphic to the dihedral group D_4. We recall that

$$D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

where r is a 90° counterclockwise rotation about the origin, and s is a reflection across the x-axis. We note that each of the elements of D_4 is a linear transformation and therefore D_4 is a transformation group.

The transformations r and s correspond to

$$r = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

By multiplying r and s, we get the following

$$e = \underline{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \quad r = \underline{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}, \quad r^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \underline{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}, \quad r^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad rS = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad r^2S = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad r^3S = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

We can see that the matrices found are identical to those in the text of the assignment. It should be emphasized that not all matrices have been evaluated here because the procedure is identical and it would take up too much space.

There we make use of the following rule:

Let G be a transformation group, and let H be the corresponding set of $n \times n$ matrices. Then H is a subgroup of $GL(n, R)$

and G and H are isomorphic

---

so, having shown that each of the matrices r, r^2, r^3 corresponds to a rotation of the plane, while each of the matrices s, rs, r^2s, r^3s corresponds to a reflection of the plane across a certain line through the origin. This gives us then that the eight matrices form a subgroup of $GL(2, \mathbb{R})$ that is isomorphic to D_4.

Problem 2 a) First we show that $\phi * \psi$ belong to $\text{Hom}(G, G')$ for all $\phi, \psi \in \text{Hom}(G, G')$, and then to show that $(\text{Hom}(G, G'), *)$ is an abelian group.

We will let a denote the first map in $\text{Hom}(G, G')$, and b denote the second map. Then for any k, d in G we have:

$a * b(k+d) =$ (by definition)

$a(k+d) +' b(k+d) =$ (since a and b are themselves)

$(a(k) +' a(d)) +'' (b(k) +' b(d)) =$ (Using the fact that G' is abelian)

$a(k) +' b(k) +' a(d) +' b(d) =$

$a * b(k) +' a * b(d)$

Hence $a * b$ itself is a homomorphism. Clearly $(a * b)$ is a map from G to G', so $a * b$ is in $\text{Hom}(G, G')$.

We now proceed to show that $(\text{Hom}(G, G'), *)$ is an abelian group. Clearly $*$ is commutative since $+'$ is commutative. The identity in $(\text{Hom}(G, G'), *)$ is just a trivial homomorphism that maps all elements of G to the identity in G'.

For any function k in $\text{Hom}(G, G')$, the inverse of k is just a function that maps all elements of G to the inverse of what the map k maps them to.

We have already shown that composition of homomorphism under $*$ yield another homomorphism, so $(\text{Hom}(G, G'), *)$ is closed. This shows that it is a group.

Problem 2b) We are going to show that $\mathrm{Hom}(\mathbb{Z}, G')$ is isomorphic to G'. We want to prove that it is a bijection and closed under operation. Because the set is finite, it is automatically closed. So, we show only the bijection.

We set $\Phi(\phi) = \phi(1)$. for $\phi \in \mathrm{Hom}(\mathbb{Z}, G')$

Because of this we can set $\phi(x) = F(\phi)\, k$. Because if $f: \mathbb{Z} \to \mathbb{Z}$ equals multiplication by k, then so does f! Because f is entirely determined by its value at 1, and since this value can be chosen arbitrarily, it is an isomorphism of $\mathrm{Hom}(\mathbb{Z}, G')$ with G'.

Problem 2c) Below we will list all the possible ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_6$. For good measure, we will also include the image and kernel for each such homomorphism.

Since $\mathbb{Z}$ is generated from 1 by addition and subtraction, if $\phi: \mathbb{Z} \to \mathbb{Z}_6$ then for any $a \in \mathbb{Z}$, we have $\phi(a) = a\phi$, where $\phi = \phi(1)$.

Then ϕ is linear, so $\phi(a) + \phi(b)$ $= ak + bk = (a+b)k = \phi(a+b)$ for any a and b in $\mathbb{Z}$.

Meaning that if ϕ is a ring homomorphism if and only if we have, for any a and b in $\mathbb{Z}$:

$$0 = \phi(ab) - \phi(a)\phi(b) = abk - (ak)(bk)$$

$$= ab(k - k^2)$$

We then take $a = b = 1$, and do

$0 = k - k^2 \bmod 6$

We have, working mod 6:

$0 - 0^2 = 0 - 0 = 0$, $1 - 1^2 = 1 - 1 = 0$,

$2 - 2^2 = 2 - 4 = -2 \neq 0$, $3 - 3^2 = 3 \cdot 9 = -6 = 0$, $4 - 4^2 = 4 - 16 = -12 \neq 0$, $5 - 5^2 = 5 - 25 = -20 \neq 0$.

The possible values of k are 0, 1, 3 and 4, and for each of these values (since $k = k^2 \bmod 6$), we have a homomorphism. Therefore, the homomorphisms are:

1) $f(a) = 0 \bmod 6$, for all $a \in \mathbb{Z}$

Image is $\{0\}$ and kernel is $\mathbb{Z}$

2) $f(a) = a \bmod 6$, for all $a \in \mathbb{Z}$

Image is $\mathbb{Z}_6$ and kernel is all

all integer multiples of 6.

3) $f(a) = 3a \bmod 6$, for all $a \in \mathbb{Z}$

The image is $\{0, 3\}$ and the kernel is all even integers

4) $f(a) = 4a \bmod 6$, for all $a \in \mathbb{Z}$.

The image is $\{0, 2, 4\}$ and the kernel is all integer multiples of 3.

Problem 3a) G is a group of order $|G| = 225$. The assignment wants us to show that G has an unique Sylow p-subgroup for each prime p that divides $|G|$, and then to explain why G is not a simple group.

A prime factorization of 225 gives

$$225 = 3^2 \times 5^2$$

The definition of a simple group G is a group with exactly two quotient groups: the trivial quotient group $\{1\} \cong G/G$ and the group $G \cong G/\{1\}$ itself.

Here we let N_p be the number of Sylow p-subgroups of G, where $p = 3$ or $p = 5$. By Sylow's Theorems, we have $N_p \equiv 1 \pmod{p}$ and $N_p \mid 3^2 5^2$.

Meaning that N_p is of the form $1+kp$ for $k = 0, 1, 2 \ldots$, and is a divisor of $3^2 5^2$. Verifying the possibilities gives us N_3 and N_5. By considering the definition of the simple group, it can be seen that G is not a simple group because it has more than two quotient groups. The other subgroups are, by Sylow's second theorem normal and they are the Sylow 3-subgroup and the Sylow 5-subgroup.

Verification of N_p. For $N_3 = \frac{3^2 5^2}{1+3k}$

$N_5 = \frac{5^2 7^2}{1+5k}$ gives us the table

$225, \frac{225}{4}, \frac{225}{7}, \frac{45}{2}, \frac{225}{13}, \frac{225}{16}, \frac{225}{19}, \frac{225}{22}, 9 \quad (k=7)$

This leads to G having a non-trivial normal subgroup, besides $N, \{1\}$

Problem 3b) We are asked to show that G is the direct product of its Sylow p-subgroups, and to show that G is abelian the first part is done by:

$$59 \cdot 25 = 225$$

$$3 \cdot 3 \cdot 25 = 225$$

$$3 \cdot 3 \cdot 5 \cdot 5 = 225$$

$$9 \cdot 5 \cdot 5 = 225$$

Let us notice M = a Sylow 3-subgroup and N = a Sylow 5-subgroup. We found in the previous assignment that M and N are normal subgroups of G. This also gives us $|M| = 3^2$ and $|N| = 5^2$ making the orders of M and N co-prime.

And because their order is of form p^2 where p is prime, both M and N are abelian. Because both M and N are abelian furthermore, it follows that their product is abelian as well.

A more precise proof could be done this way: By Sylow's theorem, any group of order 225 has an unique sylow 5-subgroup P. If this group P is cyclic, then G is abelian. We do this by choosing any sylow 3-subgroup Q and let $P = \langle a \rangle$. So, that $G = PQ$ and P and Q are abelian we prove that G is abelian by proving $ab = ba$ for any $b \in Q$. We then get $bab^{-1} = a^k$, for k since P is normal in G. $b^9 = 1$ because $|Q| = 9$. Therefore $a = b^9 a b^{-9}$ and $a^{k^9 - 1} = 1$. Giving us $k^9 \equiv 1 \mod 25$ due to the order of a

being 25. We then see that $k^9 \equiv 1 \mod 25$ has one solution, $k \equiv 1$. This makes $bab^{-1} = a^k = a$ and finally $ab = ba$. And proving that the product is abelian as well.

Problem 4 a) We let F be a field and let $F[x]$ be the ring of polynomials in one indeterminate x with coefficients in F.

a) - part of Problem 4 wants us to explain what it means for a polynomial $g(x)$ in $F[x]$ to be irreducible over F.

It means that the polynomial of degree $n \geq 1$ with coefficients in a Field F is said to be irreducible over F if it cannot be written as a product of two non-constant polynomials over F of degree less than n.

Problem 4b) We let $f(x) = x^3 + cx +$ 3. And we then proceed to find all values of c in Z_5 such that $f(x)$ is irreducible over Z_5.

We solve as following: $x^3 + x + 3$ and $f(0) = 3$; $f(1) = 4 + c = c - 1$; $f(2) = 11 + 2c = 2c - 4$; $f(3) = 30 + 3c = 3c$

$f(4) = 67 + 4c = 4c - 3$

And thereby all $f(x) \neq 0$ simultaneously. Hence, $c \neq 0, 1, 2,$ and $3/4$ (1).

As c is in Z_5, $c = 0, 1, 2, 3, 4$ (2)

From (1) and (2), we get $c = 3$ and $c = 4$.

Wolfram Alpha gives us $c = -3$ and $c = -4$ give

$f(x) = x^3 - 4x + 3$ and

$f(0) = 3$, $f(1) = 0$, $f(2) = 3$ ..., for $c = -3$, $f(2) = 5 = 0$ in Z_5. Making $k = -3$, and $c = -4$ reducible over Z_5.

Problem 4c) Here we want to find all $c \in \mathbb{Z}_5$ for which $f(x)$ is irreducible. We have already found a relevant result in Problem 4b). We use that and get that the fields in $\mathbb{Z}_5$ are:

$\mathbb{Z}_5[x]/\langle x^3+3\rangle$, $\mathbb{Z}_5[x]/\langle x^3+x+3\rangle$, $\mathbb{Z}_5[x]/\langle x^3+2x+3\rangle$, $\mathbb{Z}_5[x]/\langle x^3+3x+3\rangle$ and $\mathbb{Z}_5[x]/\langle x^3+4x+3\rangle$

are fields.

Problem 4d) In this problem we will find a basis for the field $\mathbb{Z}_5[x]/\langle f(x)\rangle$ and find the number of elements in this field.

A noted theorem says that if p is prime and $f(x) \in \mathbb{Z}_p[x]$ is irreducible then $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field since $\mathbb{Z}_p$ is a field. Furthermore, it can be shown that deg $f(x) = n$, each element of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ can be expressed uniquely as $a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 + \langle f(x)\rangle$ for some $a_i \in F$. Because there are p choices for each coefficient a_i and n coefficients, there are exactly p^n cosets of that form. $\mathbb{Z}_5[x]/\langle f(x)\rangle$ therefore is a field with $5^3 = 125$ elements.

We get that because deg $f(x) = 3$.
And Z_5 is already given.

The reference for the theorems in this text is Joseph A. Gallian and his work "Contemporary Abstract Algebra".

When it comes to the basis for a field, we need to have 1 and the roots there. So a possible basis is therefor

$$\begin{pmatrix} 1 \\ -1.2134 \end{pmatrix}$$

plus all the linear combinations of id.

Problem 5 a) $f(x) = x^3 - 5$ in $Q[x]$

with the function being a cubic polynomial we would need a zero in Z and this zero would divide 5. The possible choices are $\pm 1, \pm 2, \pm 3$. As shown below none of them lead to zeroes of $x^3 - 5$.

$1^3 - 5 = -4$	$-1^3 - 5 = -6$	$2^3 - 5 = 2$
$-2^3 - 5 = -13$	$3^3 - 5 = 22$	$-3^3 - 5 = -32$

This means that $x^3 - 5$ is irreducible over Q and that $\sqrt[3]{5}$ is irrational.

Problem 5 b) says to find the splitting field K of $f(x)$ over $\mathbb{Q}$ and the degree $[K:\mathbb{Q}]$. We remember that $f(x) = x^3 - 5$.

The splitting field K will be $\mathbb{Q}(\sqrt[3]{5}, \omega)$. K contains the cyclotomic field of third roots of unity and is generated over it by $\sqrt[3]{5}$. We therefore see that the degree is at most 6. $\mathbb{Q}(\sqrt[3]{5})$ and $\mathbb{Q}(\omega)$ are both subfields of degrees 3 and 2 respectively. Because the degrees are relatively prime, the degree must be divisible by $3 \cdot 2 = 6$ and so $[K:\mathbb{Q}] = 6$.

Problem 5c) Because this is a splitting field over $\mathbb{Q}$, the extension is normal and separable and therefore Galois. This means that the Galois has order 6.

We use the theorem below:

Let $f(x) \in K[x]$ be a separable polynomial of degree n.

a) If $f(x)$ is irreducible in $K[x]$ then its Galois group over K has order divisible by n

b) The polynomial $f(x)$ is irreducible in $K[x]$ if and only if Galois group over K is a transitive subgroup of S_n.

Here the degree $n = 3$. With $6/3 = 2$, meaning it's divisible, it also becomes a transitive subgroup of S_3. Here Cayley theorem suggests that every group G is

isomorphic to a subgroup of the symmetric group on 6, and since S_6 is precisely a symmetric group, we conclude that the Galois group $G(K/\mathbb{Q})$ is isomorphic to S_3.

Problem 5 d) The problem designs us to set up the Galois correspondence between subgroups of $G(K/\mathbb{Q})$ and subfields $\mathbb{Q} \subseteq E \subseteq K$. Furthermore we must list all the normal extensions E of $\mathbb{Q}$.

The roots are $L = \mathbb{Q}\left(\sqrt[3]{5}, \sqrt[3]{5}\,\omega, \sqrt[3]{5}\,\omega^2\right)$. The Galois group has an order of 6, as previously found. Automorphisms need to send an element to another element

that satisfies its minimal polynomial.
We can specify automorphisms by
where they could send the generators
so: $\sqrt[3]{5}$ must be sent to $\sqrt[3]{5}\mu^i$
for $i = 0, 1, 2$ (the roots of the polynomial) and μ could be sent to
μ^j, $j = 1, 2$. We get the basis
group of order 6. With the possible
indices being 1, 2, 3, 6 we get the

$$Q(\sqrt[3]{5}),\ Q(\sqrt[3]{5}\,\mu^2),$$

$$Q(\sqrt[3]{5}\,\mu^3),\ Q(\sqrt[3]{5}\,\mu^6)$$