Home-exam in MAT2200: Groups, Rings and Fields

Department of Mathematics,

University of Oslo

UiO : Universitetet i Oslo

Problem 1

a)

We shall in this first problem prove that N = $\{i, u_1, u_2, u_3\}$ is a subgroup of S_4. And to show what known group N is isomorphic to.

First, we must therefore set N as:

$$N = \big(1, (1,2)(3,4), (1,4)(2,3), (1,3)(2,4)\big)$$

One requirement for being classified a subgroup of a group is that whenever a and b are in N, then ab^{-1} is also in N.

$$\big((1,2)(3,4)\big)^2 = (1,2)(3,4)(1,2)(3,4) = (1,2)^2(3,4)^2 = 1$$

$$\big((1,4)(2,3)\big)^2 = (1,4)(2,3)(1,4)(2,3) = (1,4)^2(2,3)^2 = 1$$

$$\big((1,3)(2,4)\big)^2 = (1,3)(2,4)(1,3)(2,4) = (1,3)^2(2,4)^2 = 1$$

This means that each element is its own inverse. The following step is to show that N is closed under multiplication. We omit the comma here due to space constraints.

$$(12)(34)(14)(23) = (12)(134)(23) = (12)(2413) = (13)(24)$$

$$(12)(34)(13)(24) = (12)(143)(24) = (12)(2314) = (13)(24)$$

$$(14)(23)(12)(34) = (14)(132)(34) = (14)(3421) = (13)(24)$$

$$(14)(23)(13)(24) = (14)(123)(24) = (14)(2431) = (12)(34)$$

$$(13)(24)(12)(34) = (13)(142)(34) = (13)(3214) = (14)(23)$$

$$(13)(24)(14)(23) = (13)(124)(23) = (13)(2341) = (12)(34)$$

From this we conclude that N is closed under multiplication and N is a subgroup of S_4.

The second part of the question posed was to find what known group N is isomorphic to. We have four elements in the group giving us an order of 4. This sets a limit to what we can do next. We then have Z_4 times identity and Z_2 times Z_2. But here we must have Z_2 times Z_2 because we have identity in the set. This gives us:

$$N = Z_2 * Z_2$$

b)

Problem 1 b) asks us to prove that N is a normal subgroup of S_4. We have been given the hint that for each $\sigma \epsilon S_4$, and each transposition (i, j) in S_4, we have that:

$$\sigma(i,j) = \big(\sigma(i),\sigma(j)\big)\,\sigma$$

As mappings in S_4, where $\big(\sigma(i),\sigma(j)\big)$ as the transposition again. We will therefore follow the procedure outlined to the get the, hopefully, expected answer.

$$\big(\sigma(i,j)\big)(i) = \sigma(i,j)\ (i) = \ \sigma\ (j)$$

$$\big(\sigma(i,j)\big)(j) = \sigma\ (i,j)\ (j) = \sigma(i)$$

$$\big(\sigma(i,j)\big)(k) = \sigma(i,j)\ (k) = \sigma(k)$$

Where in the last relation k $\neq i,j$.

$$\big(\sigma(i),\sigma(j)\big)(i) = \big(\sigma(i),\sigma(j)\big)\sigma(i) = \sigma(j)$$

$$\big(\sigma(i),\sigma(j)\big)(j) = \big(\sigma(i),\sigma(j)\big)\sigma(j) = \sigma(i)$$

$$\big(\sigma(i),\sigma(j)\big)(k) = \big(\sigma(i),\sigma(j)\big)\sigma(k) = \sigma(k)$$

Where in the last relation k $\neq i,j$. So, this then leads to:

$$\sigma(i,j) = \big(\sigma(i),\sigma(j)\big)\sigma$$

And thereby:

$$\sigma(i,j)\sigma^{-1} = \big(\sigma(i), \sigma(j)\big)$$

That further becomes:

$$\sigma(i,j)\sigma^{-1} = \big(\sigma(i), \sigma(j)\big)$$

Giving us the final expression of:

$$\sigma(i,j)(k,l)\sigma^{-1} = (\sigma(i,j)\sigma^{-1})(\sigma(k,l)\ \sigma^{-1}) = \big(\sigma(i), \sigma(j)\big)(\sigma(k), \sigma(l))$$

From this we infer that N is a normal subgroup of S_4 as expected in the problem.

Problem 2

a)

We are going to show that R is a subring of $M_3(F)$. For $M_3(F)$ we refer to the text of the problem. And furthermore, we want to show that R is not commutative and does not contain unity. First some clarifications. $M_3(F)$ is the ring of 3*3 matrix over a field F. R is the subset of $M_3(F)$. So, we need to show that a ring R is a subring of $M_3(F)$, a ring in itself.

We use the definition found on the first page on the following link and try to show 1) – 4) in order to prove what we want.

http://sites.millersville.edu/bikenaga/abstract-algebra-1/ideals-and-subrings/ideals-and-subrings.pdf

1) R is closed under addition. If a, b ϵ R, then a + b ϵ R.

We have a + b, with both in R separately. So, when we take the addition of a + b, we still lack a point in the field. The full linear combination would therefore have been a + b + c, so this means that the addition of a + b is still in R, because there is an another point in addition to those two.

2) <u>The zero element of $M_3(F)$ is in R. 0 ϵ R.</u>

In the $M_3(F)$, the zero element is represented by 0i + 0j + 0k (zero multiplied by the unit vector one could also say). By putting the natural numbers (a, b, c) = (0, 0, 0), we have that the $M_3(F)$ is in R as well.

3) <u>R is closed under additive inverses, meaning that if a ϵ R, then – a ϵ R.</u>

We already know that a ϵ R. Does this mean that – a ϵ R also? We check this by looking at the determinant of a 3*3 matrix. According to this link (from Wolfram):

https://mathworld.wolfram.com/Determinant.html

when given an 3*3 determinant, the additive inverse is:

$$|-A| = (-1)^3\,|A|$$

Basically saying that, because of Cramer's rule, that a non-homogenous system of linear equations has an unique solution if the determinant of the system is non-zero. Meaning that R is closed under additive invers.

4) <u>R is closed under multiplication, if a,h ϵ R, then ab ϵ R.</u>

We have again 3 variables. One assumes for example R = a*a + a*b + a*c + b*c + b*b + c*c in a multiplication of the entire R set. This then says that R is closed under multiplication. If a, b ϵ R, then ab ϵ R as well.

Having fulfilled the four criteria we conclude that R is a subring of $M_3(F)$.

We then go on to show that R is not commutative and does not contain unity. For it to be commutative, then

$$ab = ba, for\ all\ a, b \epsilon R$$

Here we take a look at 3*3 matrix for $M_3(F)$. We see that we have an "a" in i-component position and an "a" in an j-component position. This clearly gives us that $ab \neq ba$ for all a, b ϵR.

If R has a multiplicative identity 1 = $1_R \neq 0,$ we say that R has unity. Here we see that in the matrix from the assignment of the text has a diagonal that gives 0, because it is zero in the last spot (k-component, last spot to the right). Thereby it is not unity.

b)

The question asks us to define maps ø: R -> F and ψ: R-> F. We must prove that æ is a ring homomorphism. And to evaluate whether ψ is a ring homomorphism.

Here we follow addition preserving given by:

$$ø(a + b) = ø(a) + ø(b)\ for\ all\ a\ and\ b\ in\ R$$

And multiplication preserving:

$$ø(ab) = ø(a)ø(b)\ for\ all\ a\ and\ b\ in\ R$$

and also unit (multiplicative identity) preserving. These 3 "preservations" define ring homomorphism.

So, we are that ø = a. We know that based on the matrix that we have both ø(a) + ø(a) inside of R since have a in i- and j- components. This of course also gives us multiplication preserving. We therefore have that ø is a ring homomorphism.

ψ is not a ring homomorphism because of the same argument as above.

c)

We are going to here show that the subset,

$$I = \{M(a, b, c) \in R | a = 0\}$$

is an ideal for R. And answer if I is a maximal ideal for R.

We let M (a1, b1, c1), M (a2, b2, c2) $\in I$.

And then get a1 = 0 and a2 = 0 inserted in the matrix. Then follows some calculations below:

$$M\ (a1, b1, c1) + M\ (a2, b2, c2) = M\ (0, b1 + b2, c1 + c2) \in I$$

And then we let $M(a, b, c) \in R$. Before we multiply to check if it is an ideal for R.

$$M\ (a, b, c) * M(a1, b1, c1) = M(0, ab1 + ba1, ac1) \in R$$

Therefore, it is concluded that I is an ideal of R.

We call an ideal of a ring R a maximal ideal if we cannot get any other ideals between I and R. By definition of the calculation we did above this is not possible, so this is the maximal deal of R.

Problem 3

a)

It is preliminary given that G is a group of order |G| = 1225.

We will show that G has a unique Sylow p-subgroup for each prime p that divides |G|. A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself. The order of a group, as we know, is the number of tis elements.

https://en.wikipedia.org/wiki/List_of_prime_numbers

The link above gives us precisely 200 prime numbers in the set of the group. I used MATLAB and wrote in the following to find that the 1225 is only divisible by 5 and 7, in addition to 1 and itself.

1225./primes(1225)

So, by making use of theorem 11.12 in the syllabus, we get:

$$5 * 5 * 7 * 7 = 1225$$

$$5 * 5 * 49 = 1225$$

$$25 * 7 * 7 = 1225$$

$$25 * 49 = 1225$$

And we can say that the two primes p that divide |G| can be described as 5-Sylow subgroup with order 25 and a 7-Sylow subgroup with order 49. They can be called Sylow subgroups because any subgroup of G whose order is the highest power of p dividing |G| is called a p-Sylow subgroup of G.

We were then supposed to show that G has two normal subgroups M and N such that the order of M is co-prime with the order of N. The requirement for being classified as co-prime is that 1) the only positive integer that divides both of them is 1, and 2) consequently, any prime number that divides one does not divide the other. We see that 5 and 7 are co-primes according to these two criteria. We use theorem 14.13 to show that the two normal subgroups, M and N, are 49 and 25 as seen in the calculation above. Since we have that the intersection of these subgroups must be 1, it follows that G is a direct product of the two subgroups. Again, as seen in the calculation. We then have the two groups to show that are abelian individually. The most common way is to use the theorem that: a group whose order is the square of a prime is abelian. Here we have exactly this, so they (M and N) are abelian.

Despite this not being necessary, I will provide a proof on this link:

https://kconrad.math.uconn.edu/blurbs/grouptheory/groupsp2.pdf

b)

Assignment b) wants us to show that G is isomorphic to the direct product M*N.

$$M * N = Z_M * Z_N = Z_{MN} \quad (1)$$

A theorem says that $Z_M * Z_N$ is isomorphic to Z_{MN} if M and N are co-prime. We have already proven that they are co-prime in the Problem 3 a).

The proof of this particular theorem can be found here on this link:

https://sharmaeklavya2.github.io/theoremdep/nodes/abstract-algebra/groups/isomorphism/zm-cross-zn-isomorphic-to-zmn.html

But I will rewrite it for understanding. Before that we must emphasize that we set (1) ⇔ gcd(m,n) = 1.

lcm = Lowest common multiple.

Proof of "only if" part:

$$Z_M * Z_N = Z_{MN} \;\; => Z_M * Z_N \; is \; cyclic$$

Let (a,b) be a generator of $Z_M * Z_N$. Then order ((a,b)) = MN. Let O_a = order(a) and O_b = order(b).

$$O_a \,|M \;\wedge O_b|n \qquad (Z_M \; and \; Z_N \; are \; cyclic)$$

$$=> O_a, O_b|\; lcm(m,n)$$

$$=> lcm(m,n) \; is \; a \; common \; multiple \; of \; O_a \; and \; O_b.$$

$$=> \; lcm(O_a, O_b) \leq lcm(m,n)$$

Order((a,b)) = lcm($O_a, O_b) \leq lcm(m,n) = \frac{mn}{\gcd(m,n)}$. Therefore gcd(m,n) = 1.

Proof of "if" part:

Let gcd(m,n) = 1. Let a and b be generators of $Z_M and \; Z_N$ respectively. $O_a = M \; and \; O_b = N$.

Order((a,b)) = lcm($(O_a, O_b)) = lcm(m,n) = mn/(\gcd(m,n)) \; = mn$.

$$=> Z_M * Z_N = \big((a,b)\big) \wedge |Z_M * Z_N| => Z_M * Z_N = Z_{MN}$$

By proving that M and N are co-primes and proving the actual theorem we used, we hope that it is sufficient to show that G is isomorphic to the direct product M * N.

<u>Problem 4</u>

a)

The preliminary information in this assignment is that we consider the field F = Z_3 and that we let f(x)) $x^3 + 2x + 1 \; \epsilon \; F|x|$. We must in this first assignment of problem 4 explain why:

$$K = \frac{F|x|}{<f(x)>}$$

is a field.

Before answering this problem we point to page 266 in Fraleigh, Theorem 27.25 that states that if <p(x)> is a maximal ideal in F|x|, then F|x|/<p(x)> is a field. And Theorem 27.25 further states that an ideal is maximal if and only if it is irreducible over F.

So, we understand that we need to show that f(x) is irreducible over F in the problem. We know that f(x) is given by f(x) = $x^3 + 2x + 1$.

https://www.wolframalpha.com/input/?i=x%5E3+%2B+3x+%2B2+%3D+0

We solve the function f(x) in Wolfram Alpha as seen in the link above. We see that there is no integer solution. As we recall F|x| = Z_3. Z stands for integers. We can also double check this manually with f(-1) = -2, f(0) = 1 and f(1) = 4.

This makes f(x) irreducible over F and we can therefore conclude that K is a field.

b)

$$\alpha = x + < x^3 + 2x + 1 >$$

We must use α to write a basis for K over F. And then to express $\alpha^6 \ and \ \alpha^4$ in this basis.

A basis for the question would be: (1, $\alpha, \ \alpha^2$) .

And then to express α^4 and α^6 in this basis would be:

$$\alpha^4 = -2\alpha^2 - \alpha$$

$$\alpha^6 = -2\alpha^4 - \alpha^3$$

We were required to also explain these findings of mine. The basis for α as a root of a polynomial is $\alpha^3 + \alpha + 1 = 0. \alpha^4 \ and \ \alpha^6$, one sets $\alpha^4 = \alpha^3 * \alpha \ where \ \alpha^3 = -2\alpha - 1$, and one gets the answer above.

c)

In this problem we are requested to find a monic polynomial g(x) of degree 3 in F|x| such that α^2 is a root of g(x). A monic cubic polynomial can be written in factored form:

$$(x^3 + ax^2 + bx + c) = (x - x_1)(x - x_2)(x - x_3)$$

Here I intend to let α, β, γ be the roots of the cubic polynomial and run Vieta's formula to find the elementary symmetric polynomial over $\alpha^2, \beta^2 \; and \; \gamma^2$. The elementary symmetric polynomial gives us for the third degree:

$$e_1 \, (\alpha, \beta, \gamma) = \alpha + \beta + \gamma$$

$$e_2 \, (\alpha, \beta, \gamma) = \alpha\beta + \alpha\gamma + \beta\gamma$$

$$e_3 \, (\alpha, \beta, \gamma) = \alpha\beta\gamma$$

Vieta gives us for the cubic polynomial the roots as, the polynomial is P(x) = $ax^3 + bx^2 + cx \; + d$.

$$\alpha + \beta + \gamma = \; -\frac{b}{a}$$

$$\alpha\beta + \alpha\gamma + \beta\gamma = \frac{c}{a}$$

$$\alpha\beta\gamma = \; -\frac{d}{a}$$

So, what does all this gives us? We first find the elementary symmetric polynomial for the third degree.

$$e_3 x^3 + e_2 x^2 + e_1 x + 1 = 0$$

But I want to find a monic polynomial where $\alpha^2 \; is \; a \; root$. We write this as:

$$(x^2 - \; \alpha^2) \, (x^2 - \beta^2) \, (x - \; \gamma^2)$$

$$= (x - \alpha)(x - \beta)(x - \gamma)(x + \alpha)(x + \beta)(x + \gamma)$$

$$= (x^3 + 3x + 1)(x^3 - 3x - 1)$$

Here we can use the equation f(x) because it already in F|x|. We then get an equation as:

$$x^6 - 9x^2 - 6x - 1$$

This then gives us an equation for g(x) as:

$$(x - \alpha^2)\,(x - \beta^2)\,(x - \gamma^2) = x^3 - 9x - 6 - 1$$

$$g\,(x) = x^3 - 9x - 7$$

This equation as α^2 as a root, and is in F|x|. We have included Vieta and the elementary symmetric polynomial here to show the relation between them. And then we use the fact that f(x) is already in F|x| to find g(x).

d)

Sadly could not do.

Problem 5

a)

I will here try to do a polynomial division on the equation in question, and then see if it divides. If there is no remainer, then it divides.

$$\frac{(x^5 + 2x^4 + 3x^3 + 4x^2 + 8x + 12)}{x^3 + 4} = x^2 + 2x + 3$$

We can therefore see that g(x) divides f(x) because there is no remainer.

For the second part of the question concerning the roots of f(x) in the Q-space, we have the following paragraph to muse on. According to Wolfram Alpha, f(x) becomes zero when

$$x = -2^{\frac{2}{3}}$$

This value is not a rational number (meaning that it is the fraction of two integers), so that it is not in the Quotient set of numbers. The value for when f(x) = 0, was found with Wolfram Alpha.

https://www.wolframalpha.com/input/?i=x%5E5+%2B+2x%5E4+%2B+3x%5E3+%2B+4x%5E2+%2B8x+%2B+12+%3D+0

b)

We are going to determine the splitting field L over Q. So, we need to find the roots of the polynomial $x^3 + 4$. The roots, x_1, x_2 *and* x_3, were found to be:

$$x_1 = -2^{\frac{2}{3}}$$

$$x_2 = -\left(-2^{\frac{2}{3}}\right)$$

$$x_3 = \sqrt[3]{-1}\, 2^{\frac{2}{3}}$$

This then gives us a splitting field L as:

$$L = Q\ (x_1, x_2, x_3) = Q\ \left(-2^{\frac{2}{3}}, -\left(-2^{\frac{2}{3}}\right), \sqrt[3]{-1}\, 2^{\frac{2}{3}}\right)$$

over Q. The degree can be found by multiplying 3 with 2/3 and we get 3 as the degree,

c)

Then we prove that [K:L] = 2. We first find the roots of K in order to find the splitting field K.

$$x_1 = -0.8625$$

$$x_2 = -0.4533 - 0.866i$$

$$x_3 = 0.8076 + 0.8659i$$

$$x_3 = 0.8076 - 0.6842i$$

$$x_4 = 0.8076 - 0.6842i$$

$$x_5 = 0.8076 + 0.6842i$$

If we add the five roots + identity we get a basis of 5 + 1 identity, and thereby meaning order of 6, we get roughly a degree of 6 over Q, and [K : L] therefore becomes 2. Because 6/3 = 2.

d)

The order of Galois group G is equal to the degree of extension. We previously found that the degree was 6, so therefore we have a normal subgroup with order 6.

The definition of splitting field is that it is a normal extension (reference: Syllabus). It is an algebraic extension L/K for which every polynomial that is irreducible over K has no root In L. And according to Galois theory, a normal subgroup of the Galois group occurs only if the K extension is normal. Which it is by definition, as claimed in the early parts of this paragraph. Therefore G(K/L) is a normal subgroup of the G(K/Q).

https://books.google.no/books?id=EJCSL9S6la0C&pg=PA286&lpg=PA286&dq=splitting+field+quotient+group+normal&source=bl&ots=uBYN-YtYtg&sig=ACfU3U2WBPUrwibROx58LYuNDmSheledHg&hl=no&sa=X&ved=2ahUKEwihwuGEvPHpAhWqw6YKHU3IAncQ6AEwDXoECAcQAQ#v=onepage&q=splitting%20field%20quotient%20group%20normal&f=false

Link for further references on the Galois group fundamentals.

Appendix:

In this appendix I am adding the values I got when I used the MATLAB-function in Problem 3a).

```
>> 1225./primes(1225)

ans =

 Columns 1 through 18

612.5000  408.3333  245.0000  175.0000  111.3636   94.2308   72.0588   64.4737   53.2609
42.2414   39.5161   33.1081   29.8780   28.4884   26.0638   23.1132   20.7627   20.0820

 Columns 19 through 36

18.2836   17.2535   16.7808   15.5063   14.7590   13.7640   12.6289   12.1287   11.8932
11.4486   11.2385   10.8407    9.6457    9.3511    8.9416    8.8129    8.2215    8.1126

 Columns 37 through 54

7.8025    7.5153    7.3353    7.0809    6.8436    6.7680    6.4136    6.3472    6.2183    6.1558
5.8057    5.4933    5.3965    5.3493    5.2575    5.1255    5.0830    4.8805

 Columns 55 through 72

 4.7665    4.6578    4.5539    4.5203    4.4224    4.3594    4.3286    4.1809    3.9902    3.9389
3.9137    3.8644    3.7009    3.6350    3.5303    3.5100    3.4703    3.4123

Columns 73 through 90

3.3379    3.2842    3.2322    3.1984    3.1491    3.0856    3.0549    2.9951    2.9236    2.9097
2.8422    2.8291    2.7904    2.7652    2.7283    2.6805    2.6573    2.6458

Columns 91 through 108

2.6231    2.5574    2.5154    2.4949    2.4549    2.4354    2.4067    2.3512    2.3423    2.2643
2.2395    2.1993    2.1758    2.1529    2.1454    2.1231    2.0869    2.0658

 Columns 109 through 126

2.0451    2.0383    2.0181    1.9984    1.9854    1.9790    1.9414    1.9111    1.9051    1.8934
1.8760    1.8589    1.8533    1.8202    1.8095    1.7936    1.7728    1.7475

 Columns 127 through 144
```

1.7278	1.7038	1.6850	1.6712	1.6576	1.6487	1.6312	1.6182	1.6097	1.5930
1.5847	1.5565	1.5370	1.5142	1.5105	1.4921	1.4885	1.4813		

Columns 145 through 162

1.4777	1.4601	1.4361	1.4294	1.4261	1.4195	1.3968	1.3905	1.3873	1.3811
1.3506	1.3447	1.3330	1.3186	1.3074	1.3018	1.2936	1.2854		

Columns 163 through 180

1.2668	1.2616	1.2538	1.2462	1.2361	1.2287	1.2141	1.2093	1.2022	1.1998
1.1882	1.1859	1.1790	1.1678	1.1656	1.1546	1.1524	1.1459		

Columns 181 through 198

1.1270	1.1228	1.1208	1.1167	1.1106	1.1046	1.0967	1.0908	1.0850	1.0643
1.0624	1.0533	1.0461	1.0373	1.0320	1.0268	1.0200	1.0099		

Columns 199 through 200

1.0066	1.0016