UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in:	MAT2200 — Groups, rings and fields
Day of examination:	Friday 14. June 2019
Examination hours:	9:00 – 13:00
This problem set consists of 0 pages.	
Appendices:	none
Permitted aids:	none

Please make sure that your copy of the problem set is complete before you attempt to answer anything.

Problem 1 Finite abelian groups

a

Is $\mathbb{Z}_{\geq 0}$ equipped with the operation of addition a group? Justify your answer.

Solution The set $\mathbb{Z}_{\geq 0} = \{x \in \mathbb{Z} \mid x \geq 0\}$ is not a group under the operation of addition. The element $0 \in \mathbb{Z}_{\geq 0}$ is the identity element of the operation $+$. If $x \in \mathbb{Z}$ and $x \neq 0$, then the additive inverse a of x satisfies $x + a = 0$ so that $a < 0$ and $a \notin \mathbb{Z}_{\geq 0}$. The set lacks additive inverses and therefore is not a group.

b

What are the abelian groups of order 18 up to isomorphism?

Solution By the classification theorem of finitely generated abelian groups an abelian group of order 18 must be of the form:

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \mathbb{Z}_{p_k^{r_k}}$$

where the p_i's are not necessarily distinct primes and $18 = p_1^{r_1} \dots p_k^{r_k}$. Since $18 = 2 \cdot 3^2$, there are two groups of order 18 up to isomorphism and they are,

$$\mathbb{Z}_2 \times \mathbb{Z}_9 \quad \text{and} \quad \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

c

What are the cosets of the subgroup $\langle (0,3) \rangle$ in the group $\mathbb{Z}_2 \times \mathbb{Z}_9$? Describe the quotient

$$\frac{\mathbb{Z}_2 \times \mathbb{Z}_9}{\langle (0,3) \rangle}$$

as a product of finite cyclic groups.

(Continued on page 2.)

Solution We have $H = \langle (0,3) \rangle = \{(0,0), (0,3), (0,6)\}$ and the cosets of H are

$$H, \quad (0,1)+H, \quad (0,2)+H, \quad (1,0)+H, \quad (1,1)+H, \quad (1,2)+H.$$

Therefore, the quotient group is a group of order 6. By the classification theorem of finitely generated abelian groups, there is only one abelian group of order 6 up to isomorphism, it is the cyclic group $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.

Alternatively, we can argue that $\mathbb{Z}_2 \times \mathbb{Z}_9$ is a cyclic group and any quotient of a cyclic group is cyclic. Since the order of the quotient group is 6 it is the cyclic group $\mathbb{Z}_6$.

Problem 2 Symmetric group

a

Let $\sigma = (2,6,1,4,3)$ and $\tau = (5,2,1,3)$ be permutations in S_6. Express the composition $\sigma\tau$ in disjoint cycle notation. What is the order of $\sigma\tau$?

Solution We first rewrite the composition of $\sigma\tau = (2,6,1,4,3)(5,2,1,3)$ in disjoint cycle notation as $\sigma\tau = (3,5,6,1,2,4)$. The composition consists of a single cycle of order 6. Therefore the order of $\sigma\tau$ is 6, this is the smallest positive integer such that $(\sigma\tau)^k = id$.

b

Show that if $\sigma \in S_n$ is a cycle of odd length $2k+1$ then σ^2 is also a cycle of length $2k+1$.

Solution To show that σ^2 is also a cycle of length $2k+1$, we must show that the action of $H = \langle \sigma^2 \rangle$ on $\{1, \ldots, n\}$ has one orbit of length $2k+1$ and the rest of the orbits of size 1.

Suppose the cycle is $\sigma = (a_1, \ldots, a_{2k+1})$, so that $\sigma(a_j) = (a_{j+1})$ for $j \leq 2k$ and $\sigma(a_{2k+1}) = a_1$. If $i \notin \{a_1, \ldots, a_{2k+1}\}$ then $\sigma^2(i) = \sigma(i) = i$, and $\mathcal{O}_i = \{i\}$ is an orbit of size 1. Otherwise consider $a_j \in \{a_1, \ldots, a_{2k+1}\}$, then $\mathcal{O}_{a_j} = \{(\sigma^2)^s(a_j) \mid s \in \mathcal{Z}\}$. We claim that $\mathcal{O}_{a_j} = \{a_1, \ldots, a_{2k+1}\}$. Notice that $(\sigma^2)^s(a_j) = \sigma^{2s}(a_j) = a_{j+2s}$ where $j+2s$ is considered modulo $2k+1$. Now given any $j' \in \{1, \ldots, 2k+1\}$, there exists an $s \in \mathbb{Z}$ such that congruence $j' \equiv j + 2s \mod 2k+1$ since 2 and $2k+1$ are relatively prime. Therefore, the permutation σ^2 has a single orbit of size $2k+1$ and the other orbits are of size 1. By definition σ^2 is

c

Let G be a subgroup of the symmetric group S_n such that there exist permutations $\sigma_2, \ldots, \sigma_n \in G$ satisfying $\sigma_i(1) = i$ for $2 \leq i \leq n$. Show that G acts **transitively** on the set $\{1, \ldots, n\}$. In other words, show that for each pair $1 \leq i, j \leq n$ there is a permutation $\sigma \in G$ such that $\sigma(i) = j$.

Solution For a pair i, j consider the permutation $\sigma := \sigma_j \sigma_i^{-1}$. Then $\sigma_j \sigma_i^{-1}(i) = \sigma_j(1) = j$. Therefore $\sigma(i) = j$, moreover $\sigma \in G$ since

(Continued on page 3.)

the subgroup G must contain σ_i^{-1} if it contains σ_i and it is closed under composition.

Problem 3 Rings and quotients

a

Show that if n is not a prime number, then $n\mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$.

Solution *We assume $n \neq 0$.

By definition, an ideal I of a commutative ring R is prime if for all $a, b \in R$,if $ab \in I$ then either $a \in I$ or $b \in I$.

We have $n\mathbb{Z} = \{k \in \mathbb{Z} \mid n \text{ divides } k\}$. If n is not a prime number then $n = ab$ where a and b are some other integers not equal to ± 1. Then $n = ab \in n\mathbb{Z}$ but since both a, b are not equal to ± 1, we have $a, b < n$ so n cannot divide either of them and $a, b \notin n\mathbb{Z}$. Therefore $n\mathbb{Z}$ is not prime.

b

Show that the quotient

$$\frac{\mathbb{Z}_2[x]}{\langle x^3 + x + 1\rangle}$$

is a field. How many elements does it contain?

Solution The quotient

$$K = \frac{\mathbb{Z}_2[x]}{\langle x^3 + x + 1\rangle}$$

is a field if and only if $\langle x^3 + x + 1\rangle$ is a maximal ideal of $\mathbb{Z}_2[x]$. Since $\mathbb{Z}_2$ is a field, the ideal $\langle x^3 + x + 1\rangle$ is maximal $\mathbb{Z}_2[x]$ if and only if the polynomial $x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

We first see that the polynomial has no zeros in $\mathbb{Z}_2$ since $0^3 + 0 + 1 \neq 0$ and $1^3 + 1 + 1 \neq 0$ in $\mathbb{Z}_2$. Therefore, the polynomial is irreducible since it is of degree three and any factorization over $\mathbb{Z}_2$ would consist of at least one linear factor, and hence imply it has a zero in $\mathbb{Z}_2$.

The field K is a degree 3 field extension of $\mathbb{Z}_2$ and hence it has $2^3 = 8$ elements.

c

Find a polynomial $p(x) \in \mathbb{Z}_2[x]$ such that $\deg(p(x)) \leq 2$ and

$$x^5 + \langle x^3 + x + 1\rangle = p(x) + \langle x^3 + x + 1\rangle$$

in $\frac{\mathbb{Z}_2[x]}{\langle x^3+x+1\rangle}$.

Solution The polynomial $x^2(x^3 + x + 1) \in \langle x^3 + x + 1\rangle$ Therefore,

$$x^5 + \langle x^3 + x + 1\rangle = x^5 + x^2(x^3 + x + 1) + \langle x^3 + x + 1\rangle$$

(Continued on page 4.)

and

$$x^5+\langle x^3+x+1\rangle = x^3+x^2+\langle x^3+x+1\rangle = x^3+x^2+(x^3+x+1)\langle x^3+x+1\rangle.$$

So that

$$x^5+\langle x^3+x+1\rangle = x^2+x+1+\langle x^3+x+1\rangle$$

and the polynomial $p(x)=x^2+x+1$.

Problem 4 Galois theory

a

Let K be the splitting field of the polynomial $f(x)=x^3-2\in\mathbb{Q}[x]$ over $\mathbb{Q}$. Find the degree $[K:\mathbb{Q}]$ and the Galois group $G(K,\mathbb{Q})$.

Solution Since the polynomial $f(x)$ is of degree 3, we have $[K:\mathbb{Q}]\leq 6$ and $G(K,\mathbb{Q})$ is isomorphic to a subgroup of the symmetric group S_3. The zeros of $f(x)$ are $\zeta_3^j\sqrt[3]{2}$ for $j=0,1,2$ where $\zeta_3=e^{\frac{2\pi i}{3}}$. Therefore, no roots of $f(x)$ are in $\mathbb{Q}$ and since $f(x)$ is a cubic polynomial it is irreducible over $\mathbb{Q}$.

Now the field $\mathbb{Q}(\sqrt[3]{2})$ is a simple extension of $\mathbb{Q}$ and has $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, since $f(x)$ is the irreducible polynomial of $\sqrt[3]{2}$. But the field $\mathbb{Q}(\sqrt[3]{2})$ is contained in the field of real numbers hence the other zeros $\zeta_3\sqrt[3]{2}$, $\zeta_3^2\sqrt[3]{2}$ are not in $\mathbb{Q}(\sqrt[3]{2})$.

Therefore, we have $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2})\subset K$ so $[K:\mathbb{Q}]=[K:\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3[K:\mathbb{Q}(\sqrt[3]{2})]$ Since $\mathbb{Q}(\sqrt[3]{2})\neq K$ we have $3<[K:\mathbb{Q}]$ and since $[K:\mathbb{Q}]\leq 6$ we must have $[K:\mathbb{Q}]=6$. By the Galois correspondence the group $G(K,\mathbb{Q})$ has order 6. Since it is isomorphic to a subgroup of S_3 and $|S_3|=6$, the Galois group $G(K,\mathbb{Q})$ is isomorphic to the full symmetric group.

b

Let K be the splitting field of an irreducible polynomial $f(x)\in\mathbb{Q}[x]$ of degree 3 over $\mathbb{Q}$. Let A_3 denote the alternating group, i.e. the subgroup of even permutations in S_3. Show that $G(K,\mathbb{Q})=A_3$ if and only if $K=\mathbb{Q}(\alpha)$ where α is a root of $f(x)$.

Solution Following the argument above, if $K=\mathbb{Q}(\alpha)$ where α is a root of the irreducible polynomial $f(x)$ then $[K:\mathbb{Q}]=3$ and by the Galois correspondence $|G(K,\mathbb{Q})|=3$. There is only one subgroup of S_3 of order 3 and it is the alternating group $A_3=\langle(1,2,3)\rangle$.

For the other direction suppose that $G(K,\mathbb{Q})=A_3$ then $[K:\mathbb{Q}]=3$ however for any root α of $f(x)$ we have $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$ since $f(x)$ is of degree 3 and is the irreducible polynomial of α over $\mathbb{Q}$. Therefore, $[K:\mathbb{Q}]=[K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]$ implies that $[K:\mathbb{Q}(\alpha)]=1$ and so $K=\mathbb{Q}(\alpha)$.

(Continued on page 5.)

c

Conclude that all roots of the polynomial $f(x)$ from part b) must be in $\mathbb{R}$. Hint: Use that a polynomial of odd degree with coefficients in $\mathbb{Q}$ must have at least one real root $\alpha \in \mathbb{R}$.

Solution A polynomial from part *b*) of degree 3 has Galois group $G(K, \mathbb{Q}) = A_3$ and that $K = \mathbb{Q}(\alpha)$ where α is any of is any zero of $f(x)$. A polynomial of degree 3 with coefficients in $\mathbb{Q}$ must have at least one zero in the real numbers, so we can suppose that $\alpha \in \mathbb{R}$. Then $K = \mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$ and since $\alpha, \alpha^2 \in \mathbb{R}$, we have $K \subset \mathbb{R}$. The splitting field K contains the all roots of $f(x)$, therefore all roots of $f(x)$ are real.

THE END

(Continued on page 6.)