KTH Teknikvetenskap

SF2729 Groups and Rings
Exam
Monday, March 21, 2016

Time: 08:00-13:00
Allowed aids: none
Examiner: Roy Skjelnes

Present your solutions to the problems in a way such that arguments and calculations are easy to follow. Provide detailed arguments to your answers. An answer without explanation will be given no points.

The final exam consists of six problems, each of which can give up to 6 points. The homework problems will contribute with up to 9 points on the three first problems in the exam. Credits on the three first problems in the exam will together with the contribution from the homeworks give at most 18 points.

The minimum scores required for each grade are given by the following table:

Grade	A	B	C	D	E	Fx
Credit	30	27	24	21	18	16

A score of 16 or 17 is a failing grade with the possibility to improve to an E grade by additional work.

Problem 1

Let $\Phi\colon G \longrightarrow H$ be a group homomorphism.

(a) Show that the kernel, $\ker \Phi$, is a normal subgroup. **(2 p)**

(b) Show that the image of Φ is subgroup. Is it normal? **(2 p)**

(c) For any $a \in G$, show that the order of $\Phi(a)$ divides the order of a. **(2 p)**

Solution

1. The kernel always contains the identity element e, so its non-empty. Let a, b be elements in the kernel. We have that ab^{-1} is in the kernel since $\Phi(ab^{-1}) = \Phi(a)\Phi(b)^{-1} = e \cdot e^{-1} = e$. Therefore the kernel is a subgroup. We need to check normality. Let x be any element of G. The element xax^{-1} is mapped to $\Phi(x)e'\Phi(x)^{-1}$, where e' is the identity element in H. We get that $\Phi(x)e'\Phi(x)^{-1} = \Phi(x) \cdot \Phi(x)^{-1} = e'$, and the kernel is normal.

2. The image is a subgroup: Its non-empty and if we have any elements a, b in the image, let a', b' be elements in their pre-image. We then have that $ab^{-1} = \Phi(a')\Phi(b')^{-1} = \Phi(a'b'^{-1})$. This is not necessarily normal since there exist subgroups that are not normal. Take for instance the group of two elements $G = S_2$ embedded as the permutations of the first two letters in S_3. Then G as well as its image is generated by (12) which is not normal as all transpositions in S_3 are conjugated.

3. Let n be the order of the element $a \in G$. Then $a^n = e$, and so $\Phi(a)^n = e'$ and the order of $\Phi(a)$ divides n.

Problem 2

Let R be a commutative ring with 1.

(a) Define what an nilpotent element is, and show that the set of nilpotent elements in R form an ideal. **(2 p)**

(b) Show that if an element $x \in R$ is nilpotent, then x is contained in any prime ideal of R. **(2 p)**

(c) Give an example of a ring R that is not an integral domain, and has no nilpotent elements other than zero. **(2 p)**

Solution

1. An element $x \in R$ is nilpotent if $x^n = 0$ for some $n \geq 0$. If x is nilpotent, then clearly rx is nilpotent for any $r \in R$. Moreover, if x and y are nilpotent, then $(x+y)$ is also nilpotent: Let n be such that $x^n = 0$, and m such that $y^m = 0$. Then we expand

$$(x+y)^N = \sum_{i=0}^{N} \binom{N}{i} x^i y^{N-i}.$$

Let $N \geq 2 \cdot \max\{n, m\}$, and we see that $(x+y)^N = 0$.

2. Let P be a prime. Let x be nilpotent. We then have that $x^n = 0 \in P$. Let n be the smallest integer such that $x^n \in P$, but where x^{n-1} not in$P$. This integer exists. We then have that $x^n \in P$, and since P is prime we get that $x \in P$ or $x^{n-1} \in P$. It follows that $x \in P$ since $x^{n-1} \in P$ would contradict our assumption on n.

3. For instance $\mathbb{Z}/(6)$, has zero divisors, but no other nilpotents than 0.

Problem 3

(a) Describe the irreducible factors of the monic polynomial **(3 p)**

$$f(x) = x^5 - x^4 + 3x^3 + 3x^2 - 3x - 3 \quad \text{in} \quad \mathbb{Q}[x].$$

(b) Let $F(x) = (x - a_1) \cdots (x - a_n)$ be a polynomial with distinct roots $a_i \neq a_j$ (when $i \neq j$) in $\mathbb{Q}$. Show that **(3 p)**

$$\mathbb{Q}[x]/(F(x)) \simeq \prod_{i=1}^{n} \mathbb{Q}.$$

Solution

1. We see that 1 is a root of $f(x)$ since $f(1) = 0$. Polynom division then gives that $f(x) = (x^4 + 3x^3 + 6x + 3)(x - 1)$. The polynomial $x^4 + 3x^2 + 6x + 3$ is irreducible in $\mathbb{Z}[x]$ by the Eisenstein criterion, $p = 3$. Hence irreducible in $\mathbb{Q}[x]$.

2. For any $a \in \mathbb{Q}$ we have that $(x - a)$ is irreducible, hence a maximal ideal. Different maximal ideals are co-prime. By the Chinese Restminder Theorem we obtain the equality of ideals

$$(x - a_1) \cdots (x - a_n) = \cap_{i=1}^{n} (x - a_i).$$

The canonical map

$$\varphi \colon \mathbb{Q}[x] \to \prod_{i=1}^{n} \mathbb{Q}[x]/(x - a_i)$$

then has kernel $(x-a_1)\cdots(x-a_n)$, which clearly equals the ideal $(F(x))$. And we have that $\mathbb{Q}[x]/(x-a) = \mathbb{Q}$.

Problem 4

Let $G = \mathrm{GL}_2(\mathbb{Z}_3)$ the group of invertible (2×2)-matrices with entries in the field with three elements. The group acts naturally on the vector space $\mathbb{Z}_3^2$, and also on the set L of lines that passes through origin.

(a) Determine the order of G. **(2 p)**

(b) Show that the center of G is the set of scalar matrices, and isomorphic to S_2. **(2 p)**

(c) Show that the action of G on the set L induces a surjective group homomorphism from G to S_4; the symmetric group in four letters. **(2 p)**

Solution

1. The first row in the matrix can be any non-zero vector in $\mathbb{Z}_3^2$. Given the first row, the condition on the second row is that it is not a scalar multiple of the first. Therefore we get that the number of elements in G is $(3^2-1)(3^2-3) = 8 \cdot 6 = 48$.

2. Let $Z(G)$ denote the center, and let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element. Then in particular we have that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}.$$

   So $b = c$ and $a = d$. We also have that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} a & -b \\ c & -d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ -c & -d \end{bmatrix},$$

   so $b = 0$ and $c = 0$. We then have that the center $Z(G)$ is a subset of the scalar matrices. However, the scalar matrices do commute, so $Z(G)$ equals the scalar matrices. We have only two elements, the identity matrix and -1 times the identity matrix in the zenter, so the group $Z(G)$ is S_2.

3. A line passing through origo is given by a non-zero vector. Two non-zero vectors determine the same line if they are equal up to a scalar. Therefore we have four lines passing through origo. We identify the set L with the four numbers $1, 2, 3, 4$ by marking the lines. The natural action of G on L determines a group homomorphism $\Phi\colon G \to S_4$, sending $g \in G$ to the permutation $\Phi(g) = \mu_g$ where $\mu_g(l) = g \cdot l$, where l is any number/line in L. The kernel of the induced group homomorphism are those elements that act trivially on L, that is

$$\mu_g(l) = g \cdot l = l,$$

for all lines $l \in L$. Thus, the kernel is the set of scalar matrices $Z(G) = \ker(\Phi)$. The image of Φ is then a subgroup of order $48/2 = 24 = |S_4|$, and it follows that Φ is surjective.

Problem 5

Let $R = \mathbb{Z}[\sqrt{7}] = \mathbb{Z}[x]/(x^2 - 7)$, which is a free $\mathbb{Z}$-module of rank 2. Let $N\colon R \to \mathbb{Z}$ be the map $N(a + bx) = a^2 - 7b^2$. Then N is multiplicative.

(a) Determine a unit ξ, different from ± 1. **(1 p)**

(b) Show that $(2 + x)$ and $(2 - x)$ are co-prime.[1] **(2 p)**

(c) Write 6 as a product of irreducibles, and verify if any of these irreducible components are associates **(3 p)**

Solution

1. We need to find a solution to $a^2 - 7b^2 = \pm 1$. One solution is $\xi = 8 + 3x$, which has norm $8^2 - 7 \cdot 3^2 = 1$.

2. By substituting $x = 2$ in the quotient ring $\mathbb{Z}[x]/(x^2 - 7, x - 2)$ we obtain that it is the field $\mathbb{Z}/(3)$. So $x - 2$, and similarily $x + 2$ is a maximal ideal. These two maximal ideals are not associates. Because, assume that we have $a + bx$ such that

$$2 + x = (2 - x)(a + bx) = 2a - 7b + x(2b - a).$$

   This is an equality that requires $1 = 2b - a$, so $a = 2b - 1$. And we also have that $2a - 7b = 2$ which gives $2 = 4b - 2 - 7b = -2 - 3b$, which has no integer solution.

3. We have $6 = 2 \cdot 3$. We have that $2 = (3+x)(3-x) = 9-7$ and that $3 = (2+x)(-1)(2-x) = -(4 - 7)$. The norm of $3 + x$ and $3 - x$ is two, which is a prime, hence these two elements are irreducible. Similarily, the norm of $2 + x$ and $2 - x$ is -3, and these two elements are also irreducible. Therefore we have a decomposition into irreducibles as

$$6 = (3 + x)(3 - x)(2 + x)(-2 + x).$$

   Two associate elements must have $\pm$ the same norm. So the question is wheter $3 + x$ is associate to $3 - x$, and if $2 + x$ is associate to $2 - x$. We have from the results above that $2 + x$ is not associate to $2 - x$. However, we have that $(3 - x) \cdot (8 + 3x) = 24 - 21 - 8x + 9x = 3 + x$. The element $8 + 3x$ is a unit, so these two elements are associates.

[1] Co-prime is the same as co-maximal.

Problem 6

Let $\mathbb{Q}$ denote the rational numbers, which is an abelian group under addition.

(a) Show that $\mathbb{Q}$ is not a finitely generated group. **(2 p)**

(b) Show that $\mathrm{Aut}(\mathbb{Q})$ is isomorphic to $\mathbb{Q}^*$; the multiplicative group of the non-zero rational numbers. **(2 p)**

(c) Show that $\mathrm{Aut}(\mathbb{Q}^2)$ is isomorphic to $\mathrm{GL}_2(\mathbb{Q})$. **(2 p)**

Solution

1. Suppose the group was finitely generated, and let $x_1, \ldots, x_n$ be a set of generators. Then any element in $\mathbb{Q}$ can be written as $a_1x_1 + \cdots + a_nx_n$, with integers $a_1, \ldots, a_n$. Assume that the rational numbers $x_i = n_i/m_i$ are written in reduced form, and let m be the least common multiple of their deonominators. Let p be a prime number which is not a divisor of m. Then, by assumption the rational number $1/p = \sum_{i=1}^n a_i x_i$. This is however impossible because
$$\sum_{i=1}^n a_i x_i = \sum_{i=1}^n \frac{a_i n_i}{m_i} = \frac{1}{m}\sum_{i=1}^n a_i' n_i = \frac{a}{m},$$
and we have assumed that p does not divide m.

2. Let φ be an automorphism, and set $a = \varphi(1)$. Then $\varphi(n) = n\varphi(1)$. We then get that $a = \varphi(1) = \varphi(n \cdot 1/n) = n \cdot \varphi(1/n)$, and that $\varphi(1/n) = a/n$. Thus any automorphism is determined by the number $\varphi(1)$, and the only number we can not allow is $a = 0$. This shows that $\mathbb{Q}^*$ is the set of automorphisms. The composition is identified with multiplication, and it follows that the groups are isomorphic.

3. Let Φ be an automorphism of $\mathbb{Q}^2$. Let $\Phi(1,0) = (a,b)$ and $\Phi(01,) = (c,d)$. Argueing as above shows that these two values determine the automorphism. For any $(x,y) \in \mathbb{Q}^2$ we get that
$$\Phi(x,y) = x\Phi(1,0) + y\Phi(0,1) = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$
We then have that any automorphism Φ determines a matrix, and that composition is identified with matrix multiplication. The matrix represents a $\mathbb{Q}$-linear map, and such a map is a bijection if and only if the matrix is invertible. This show that the group of automorphisms equals $\mathrm{GL}_2(\mathbb{Q})$