KTH Teknikvetenskap

SF2729 Groups and Rings
Final Exam
Wednesday, May 26, 2010

Time: 08.00-12.00
Allowed aids: none
Examiner: Mats Boij

This final exam consists of two parts; Part I (groups part) and Part II (rings part). The final credit for Part I will be based on the maximum of the results on the midterm exam and Part I in the final exam.

Each problem can give up to 6 points. In the first problem of each part, you are guaranteed a minimum given by the result of the corresponding homework assignment. If you have at least 2 points from HW1, you cannot get anything from Part a) of Problem 1 of Part I, if you have at least 4 points from HW1 you cannot get anything from Part a) or Part b) of Problem 1 of Part I. Similarly for HW2 and Problem 1 of Part II.

The minimum requirements for the various grades are according to the following table:

Grade	**A**	**B**	**C**	**D**	**E**
Total credit	30	27	24	21	18
From Part I	13	12	11	9	8
From Part II	13	12	11	9	8

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 give no points.

PART I - GROUPS

(1) (a) Show directly from the axioms that there is a unique group with three elements up to isomorphism. **(2)**

(b) Show that the group $\mathrm{Gl}_2(\mathbb{F}_2)$ of invertible 2×2-matrices over the field $\mathbb{F}_2 = \{0, 1\}$ is isomorphic to the symmetric group S_3 by giving an explicit isomorphism. **(2)**

(c) Compute the center of the general linear group $\mathrm{Gl}_n(\mathbb{C})$, i.e., the group of invertible complex $n \times n$-matrices. **(2)**

(2) (a) Define what it means for a group to act on a set and show that any group acts on itself by conjugation, i.e., by $a.b = aba^{-1}$, for $a, b \in G$. **(2)**

(b) Use 2a to prove the *class equation* for a finite group G, i.e.,

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|}$$

where $C_G(a) = \{b \in G | ab = ba\}$ and $a_1, a_2, \ldots, a_r$ are representatives of all the non-trivial conjugacy classes in G. **(2)**

(c) Use the class equation to show that any non-abelian group of order $2p$, where p is an odd prime, has p elements of order 2 and $p - 1$ elements of order p. **(2)**

(3) (a) An *automorphism* of a group G is an isomorphism from G to itself. Show that the set $\mathrm{Aut}(G)$ of automorphisms of G forms a group under composition. **(2)**

(b) Show that the set $\mathrm{Inn}(G)$ of *inner automorphisms*, i.e., $a \mapsto bab^{-1}$, for some b in G, forms a subgroup of $\mathrm{Aut}(G)$. **(2)**

c) Determine the automorphism group of the non-cyclic group of order 4. **(2)**

PART II - RINGS

---

(1) Consider the ring $R = \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

(a) Compute its characteristic, $\mathrm{char}(R)$. **(2)**

(b) Show that $R \cong \mathbb{Z}_{60} \times \mathbb{Z}_3$ as rings. **(2)**

(c) Let R be a commutative ring with unity and let I and J be two ideals in R satisfying $I + J = R$ and $I \cap J = (0)$. Show that $R \cong R/I \times R/J$. **(2)**

---

(2) Consider the polynomial $p(x) = x^3 + 2x^2 - 5x - 3$ as a polynomial in the polynomial rings $\mathbb{Q}[x]$ and $\mathbb{Z}_5[x]$, and let $R = \mathbb{Q}[x]/(p(x))$ and $S = \mathbb{Z}_5[x]/(p(x))$.

(a) Show that R is a vector space over $\mathbb{Q}$ and that S is a vector space over $\mathbb{Z}_5$. What are the dimensions of these vector spaces? **(2)**

(b) Determine whether R and/or S are integral domains or even fields? **(2)**

(c) Show that R/P is a field whenever R is a PID and P is a prime ideal in R. **(2)**

---

(3) Recall that a field extension L of a field F is called a splitting field of $f(x)$ over F if the following holds:

(i) $f(x)$ splits as a product of linear factors in $L[x]$.

(ii) If $L' \subseteq L$ is another extension such that $f(x)$ splits as a product of linear factors in $L'[x]$, then $L' = L$.

(a) Show that $\mathbb{Q}(i)$ is a splitting field of $x^2 - 2x + 2$ over $\mathbb{Q}$. **(2)**

(b) Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial of degree 2. Show that $F[x]/(f(x))$ is a splitting field of $f(x)$ over F of degree 2. **(2)**

(c) Give an example of a field F and an irreducible polynomial $p(x) \in F[x]$ of degree 3 such that $F[x]/(p(x))$ is not a splitting field for $f(x)$ over F. **(2)**
