LUNDS TEKNISKA HÖGSKOLA
MATEMATIK

TENTAMENSSKRIVNING
ALGEBRA
2007-05-28 – 2007-06-07

Any "non-human" aids are permitted, but complete solutions should be included. Write your name, section-year (subject for PhD-students), id-number and email address on the first page, and write your name on each of the following pages.

1. a) Construct an RSA crypto system using the primes $p = 37$ and $q = 43$. (With notations in Hungerford, determine n, k, d and e.) Use your system to encode 10+your birth date. (Born Feb 24th $\Longrightarrow$ encode 34.) (0.6)

b) You are given the public key $N = 391$ and $e = 19$ of an RSA system. Break the system, i.e. find d. (0.4)

2. Let $K = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$.

a) Show that K is a field. (0.2)

b) Let α be a root of $x^3 + x^2 + 1$ in K. Show that $\alpha^6 = \alpha^2 + \alpha$ in K. (0.4)

c) Find the inverse of α^6 in K. (0.4)

3. a) Let G be a group that has elements of every order from 1 through 15. Find the smallest possible value of $|G|$. (0.5)

b) Let G be a finite group and let H be a subgroup such that $H \subseteq Z(G)$ and $[G : H] = p$, p prime. (As usual, $Z(G)$ denotes the center of G.) Prove that G is abelian. (0.5)

4. Let $K \subseteq L \subseteq N$ be fields and $\alpha \in N$. Assume that

$$m = [L : K], \qquad n = [K(\alpha) : K]$$

are finite and relatively prime. Show that

$$[L(\alpha) : K] = mn.$$

5. a) An element $a \in R$ (ring) is called *nilpotent* if $a^n = 0_R$ for some positive integer n. Let N denote the set of all nilpotent elements in a commutative ring R. Show that N is an ideal in R. (0.3)

b) For R and N in **a)**, prove that $N \subseteq P$ for every prime ideal P in R. (0.3)

c) Let R be a commutative ring with unity and assume that there for every $a \in R$ is an integer $n \geq 2$ such that $a^n = a$. Show that every prime ideal in R is maximal. (0.4)

6. Let G be a group with $|G| = p^2$, p prime.

a) Prove that G can be generated by two elements. (0.3)

b) Prove that G has a normal subgroup of order p. (0.5)

c) Prove that G is abelian. (0.2)