Uppsala universitet
Matematiska institutionen
Ernst Dieterich

Kandidatprogrammet i matematik
Autumn term 2014

Prov i matematik
Algebraic structures, 10hp
2015–08–25

Skrivtid: 14.00–19.00. Inga hjälpmedel förutom skrivdon. Lösningarna skall åtföljas av förklarande text. Varje uppgift ger maximalt 5 poäng.

1. Let $\mathrm{D}_6 = \langle \varrho, \sigma \mid \varrho^6 = e = \sigma^2, \sigma\varrho\sigma^{-1} = \varrho^{-1} \rangle$ be the dihedral group of order 12.

(a) Find the orders of the cyclic subgroups $\langle \varrho \rangle < \mathrm{D}_6$ and $\langle \varrho^i \sigma \rangle < \mathrm{D}_6$, for all $0 \leq i \leq 5$.

(b) Which of the subgroups in (a) is normal in D_6, and which is not? Give reasons for your answer!

2. Show that every abelian group of order 2310 is cyclic.

3. (a) Prove that every complex number α is algebraic over $\mathbb{R}$.

(b) Show that the quotient ring $\mathbb{R}[X]/(\mathrm{irrpol}_{\mathbb{R}}(\alpha))$ is isomorphic to $\mathbb{C}$, whenever $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

(c) Prove that the quotient rings $\mathbb{R}[X]/(X^2+aX+b)$ and $\mathbb{R}[X]/(X^2+cX+d)$ are isomorphic, whenever $a, b, c, d \in \mathbb{R}$ satisfy $a^2 < 4b$ and $c^2 < 4d$.

4. Find the addition table and the multiplication table of a field of order 4.

5. (a) Let K be a field, and let $f(X)$ be a nonconstant polynomial in $K[X]$. When is $f(X)$ called *separable*? Reproduce the definition!

(b) Let $p(X)$ and $q(X)$ be polynomials in $K[X]$ that both are monic, irreducible and separable. Assume moreover that $p(X) \neq q(X)$. Is $f(X) = p(X)q(X)$ separable? Proof or counterexample!

Please turn over!

6. Given $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + X^5 \in \mathbb{Z}_5[X]$, prove the following assertions.

(a) If $a_1 = a_2 = a_3 = a_4 = 0$, then $f(X)$ is not irreducible in $\mathbb{Z}_5[X]$.

(b) If $f(X)$ is irreducible in $\mathbb{Z}_5[X]$, then $f(X)$ is separable.

7. Explain why the problem of doubling the cube is not solvable by ruler and compass.

8. (a) What is meant by a *Galois extension*? Reproduce the definition!

(b) Let $\mathbb{A}$ be the field of all algebraic numbers. Show that $\mathbb{Q} \subset \mathbb{A}$ is a Galois extension.

(c) If $\mathbb{Q} \subset E \subset \mathbb{A}$ is an intermediate field, then every field morphism $\varphi : E \to \mathbb{A}$ can be extended to a field morphism $\psi : \mathbb{A} \to \mathbb{A}$. Use this fact to show that the Galois group $\mathrm{Gal}(\mathbb{A}/\mathbb{Q})$ is infinite.

GOOD LUCK!