Uppsala universitet
Matematiska institutionen
Ernst Dieterich

Kandidatprogrammet i matematik
Autumn term 2011
16/11/2011

Algebraic structures

Fifth sheet of exercises

56. If K is a field and $q(X) \in \operatorname{irr}(K[X])$, then $E = K[X]/(q)$ is a field extension of K. Show that $E = K[\alpha] = K(\alpha)$, where $\alpha = X + (q) \in E$.

57. Find all ideals in $\mathbb{R}^{n\times n}$, for any $n \in \mathbb{N} \setminus \{0\}$.

58. We know that if $K = (K, +, \cdot)$ is a field, then both $(K, +)$ and $(K \setminus \{0\}, \cdot)$ are abelian groups. Suppose conversely that a set K is equipped with an abelian group structure $+$ on K and an abelian group structure $\cdot$ on $K \setminus \{0\}$. Which additional requirements must $(K, +, \cdot)$ satisfy to make sure that $K = (K, +, \cdot)$ is a field?

59. Show that a commutative ring is a field if and only if it has precisely two ideals.

60. Show that every field is a principal ideal domain which has no irreducible elements. Is every field a unique factorization domain?

61. Let R be a domain. Prove the following statements.

(a) $R[X]$ is a domain.

(b) $R^\iota = R[X]^\iota$.

(c) $\operatorname{irr}(R) \subset \operatorname{irr}(R[X])$.

62. Let $n = \prod_{i=1}^{\ell} p_i$, where $p_1, \ldots, p_\ell$ are distinct prime numbers. Show that the real number $\sqrt[m]{n}$ is not rational, for all $m \geq 2$.

63. Let K be a field of characteristic not 2. Show that the polynomial $X^2 + Y^2 - 1$ is irreducible in $K[X, Y]$.

64. Prove the following so-called *universal property of the polynomial ring*. Let $\varphi : R \to S$ be a morphism of commutative rings, and let $s \in S$. Then φ extends uniquely to a ring morphism $\varphi_s : R[X] \to S$ with $\varphi_s(X) = s$, namely $\varphi_s\left(\sum a_i X^i\right) = \sum \varphi(a_i) s^i$.

65. Let R be a commutative ring, and let $a \in R$. Show that the *substitution map*

$$\sigma_a : R[X] \to R[X],\ \sigma_a(f(X)) = f(X + a)$$

is a ring automorphism.

Please turn over!

66. Let R be a commutative ring, let $f(X) \in R[X]$ and $a \in R$. Prove that $f(X) \in \mathrm{irr}(R[X])$ if and only if $f(X+a) \in \mathrm{irr}(R[X])$.

67. Decide whether or not the following polynomials are irreducible in $\mathbb{Z}[X]$.

(a) $f(X) = 1 + X^4$.

(b) $g(X) = 1 + X^3 + X^6$.

68. Let p be a prime number. Prove that p divides $\binom{p}{i}$ for all $0 < i < p$.

69. Let K be a field of prime characteristic p. Prove that the following identities hold for all $a, b \in K$ and all $n \in \mathbb{N}$.

(a) $(a+b)^p = a^p + b^p$.

(b) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

(c) $(a-b)^{p^n} = a^{p^n} - b^{p^n}$.

70. Prove that for each prime number p the p-th cyclotomic polynomial

$$\Phi_p(X) = 1 + X + X^2 + \ldots + X^{p-1}$$

is irreducible in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$.

71. Show that $[\mathbb{R} : \mathbb{Q}] = \infty$.