Indian Institute of Technology Kanpur
Department of Mathematics and Statistics

Abstract Algebra (MTH 204A/B)

Exercise Set 5

(1) Show that the following is a subring of $\mathbb{R}[[x]]$: $\left\{\sum_{k=0}^{\infty} a_k x^k : a_k \in \mathbb{R}, \forall k \geq 0 \text{ and } \sum_{k=0}^{\infty} |a_k| < \infty\right\}$.

(2) Find all intermediate rings between $\mathbb{R}$ and $\mathbb{C}$.

(3) Let R stand for the ring of all Cauchy sequences in $\mathbb{Q}$. Show that the following is a maximal ideal of R:

$$\left\{\{a_n\}_{n=1}^{\infty} \in R : \lim_{n\to\infty} a_n = 0\right\}.$$

(4) (a) Show that, given any commutative ring R with unity, there is a unique ring homomorphism from $\mathbb{Z}$ to R. The unique nonegative generator of iits kernel is called the *characteristic* of R.
(b) Let R be as above in (4a). If R is a field in addition then show that R is an extension of either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, for some prime p.
(c) Let R be a commutative ring with unity whose charactreristic is p, where p is a prime. Show that $R \longrightarrow R$, $a \mapsto a^p, \forall a \in R$, is an endomorphism. This homomorphism is called *Frobenius endomorphism* of R.

(5) (a) Find all endomorphisms of $\mathbb{R}$.
(b) Find all endomorphism φ of $\mathbb{C}$ such that $\varphi(x) = x$, for all $x \in \mathbb{R}$.

The following exercises (6)-(9) aim to show the irreducibility of the *cyclotomic* polynomials $\Phi_n(x)$ (defined in (8)), where $n \in \mathbb{N}$.

(6) Let $\mathbb{F} \subseteq \mathbb{K}$ be an extension of fields and $f, g \in \mathbb{F}[x]$ with $f \neq 0$. Show that the division with remainder of g by f gives the same answer, whether carried out in $\mathbb{F}[x]$ or in $\mathbb{K}[x]$. Deduce that $f(x)|g(x)$ in $\mathbb{K}[x] \iff f(x)|g(x)$ in $\mathbb{F}[x]$.

(7) Let $\mathbb{F}$ be a field and $f(x) := a_0 + a_1x + \cdots + a_kx^k \in \mathbb{F}[x]$, where $k \in \mathbb{N}$. We define the *derivative* of f formally as

$$a_1 + 2a_2x + \cdots + ka_kx^{k-1},$$

and denote by $f'(x)$. Show that $f(x)$ has no repeated root in $\mathbb{F}$ if and only if $\gcd(f(x), f'(x)) = 1$.

(8) Let $n \in \mathbb{N}$ and $\mu_n := \{z \in \mathbb{C} : z^n = 1\}$. We say $\omega \in \mu_n$ a *primitive* n-th root of unity if $\langle\omega\rangle = \mu_n$. Define

$$\Phi_n(x) := \prod_{\langle\omega\rangle=\mu_n} (x - \omega).$$

Note that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Show that $\Phi_n(x)$ is a monic polynomial of degree $\varphi(n)$ with integral coefficients. (Hint: Use induction and then Gauss lemma.)

(9)∗ Show that, for any $n \in \mathbb{N}$, $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible following the steps given below:
(a) Assume the contrary. Show that there exist monic polynomials $f(x)$ and $g(x) \in \mathbb{Z}[x]$ such that $\Phi_n(x) = f(x)g(x)$ and $f(x)$ is irreducible.
(b) Let ω be a root of $f(x)$ and p be a prime not dividing n. Show that $f(\omega^p) = 0$. (Hint: Otherwise $g(\omega^p) = 0$. This means ω is a root of the polynomial $g(x^p)$. This implies that $g(x^p) = f(x)h(x)$, for some $h(x) \in \mathbb{Z}[x]$. Reducing both sides modulo p, one obtains that $\bar{f}$ and $\bar{g}$ have a common factor in $\mathbb{Z}/p\mathbb{Z}[x]$. It follows now that $\bar{\Phi}_n(x)$ has a repeated root over $\mathbb{Z}/p\mathbb{Z}$. Now show that this is not possible.)

(c) Every primitive n-th root of unity is a root of $f(x)$. Conclude now that $f(x)$ has to be $\Phi_n(x)$.

(10) Find all automorphisms of $\mathbb{Q}[\omega]$ and $\mathbb{Z}[\omega]$, where ω is an n-th root of unity.

(11) Let $\mathbb{F}$ be a field. Find the field of fractions of $\mathbb{F}[[t]]$.

(12) Consider the natural inclusion $\mathbb{C} \hookrightarrow \mathbb{C}[t]$ and let φ be its unique extension to $\mathbb{C}[x, y]$ with $x \mapsto t+1$ and $y \mapsto t^3 - 1$. Find $\ker \varphi$ and show that every ideal of $\mathbb{C}[x, y]$ that contains $\ker \varphi$ can be generated by two elements.

(13) Let G be a finite group having a finite dimensional irreducible representation ρ of degree n and character χ.
   (a) Show that $\forall g \in Z(G)\, \exists \lambda_g \in \mathbb{C} \setminus \{0\}$ such that $\rho(g) = \lambda_g I$. Find $|\chi(g)|$ when $g \in Z(G)$.
   (b) Show that n can not exceed the square root of the number of inner automorphisms of G.
   (c) If ρ is *faithful*, i.e., ρ is injective, then show that $Z(G)$ is cyclic.

(14) Let G be a finite abelian group. Recall the irreducible character of G can be identified with homomorphisms from G to $\mathbb{S}^1$ and, the set of all irreducible characters of G forms an abelian group of order $|G|$ with respect to pointwise multiplication. We call this group as the *dual group* of G and denote by $\hat{G}$. For each $g \in G$, consider the following map:

$$\xi_g : \hat{G} \longrightarrow \mathbb{C} \setminus \{0\},\ \xi_g(\chi) = \chi(g), \text{ for all } \chi \in \hat{G}. \qquad (*\ 1)$$

   (a) Show that each ξ_g defined above in $(*\ 1)$ is an irreducible character of $\hat{G}$.
   (b) Prove the version of the *Pontryagin duality* for finite abelian groups which is as follows:

$$G \longrightarrow \hat{\hat{G}},\ g \mapsto \xi_g \text{ is an isomorphism.}$$