HOMEWORK 8

Due date: Tuesday of Week 9

Exercises: 3.2, 3.3, 3.4, 3.6, 3.9, 3.10, 4.1, 4.2, 7.3, 7.4, 7.5, 7.8, 7.10 Pages 472-474, Artin's book.

Here is a reminder of the following important result.

Theorem 0.1 (Hoffman-Kunze, page 266)**.** *Let F be a field of characteristic zero. Given a nonconstant polynomial $f \in F[x]$. TFAE*

1. *f is a product of distinct irreducible polynomials;*
2. *$gcd(f, f') = 1$;*
3. *f has no repeated roots in any field extension K/F.*

Problem 1. *Let K/F be a field extension. Given $f, g \in F[x] \subset K[x]$ with $f \neq 0$. Show that*

1. *Division with remainder of g by f in $F[x]$ is the same as that in $K[x]$. More precisely, if $g = fq_0 + r_0$ and $g = fq + r$ with $q_0, r_0 \in F[x]$, $q, r \in K[x]$ and $\deg(r_0) < \deg(f)$ and $\deg(r) < \deg(f)$, show that $q_0 = q$ and $r_0 = r$;*
2. *$f|g$ in $K[x]$ iff $f|g$ in $F[x]$;*
3. *$gcd_F(f, g) = gcd_K(f, g)$;*
4. *If f, g have a common root in K then $gcd_F(f, g) \neq 1$;*
5. *if $gcd_F(f, g) \neq 1$, then there exists a field extension L/F such that f, g have a common root in L;*
6. *If f is irreducible and f, g have a common root in K, then $f|g$.*

This is Proposition 15.6.4.

1. Trace, norm and minimal polynomial

Let K/F be a finite field extension. We view K as a finite dimensional vector space over F. For $\alpha \in K$, consider the linear map $T_\alpha : K \to K$ defined by $T_\alpha(x) = \alpha x$. Then T_α is F-linear and thus it determines a matrix in $\mathrm{Mat}_{n\times n}(F)$. Here $n = \dim_F K$. We can consider the trace, determinant, minimal polynomial, characteristic polynomial of T_α.

Definition 1. For $\alpha \in K$, we define

$$\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}(T_\alpha),$$

and

$$\mathrm{Nm}_{K/F}(\alpha) = \det(T_\alpha).$$

The element $\mathrm{Tr}_{K/F}(\alpha) \in F$ is called the trace of α and $\mathrm{Nm}_{K/F}(\alpha) \in \alpha$ is called the norm of α (with respect to the field extension K/F).

Problem 2. *Given $c \in F, \alpha, \beta \in K$.*

1. *Show that* $\mathrm{Tr}_{K/F}(c\alpha + \beta) = c\mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$.
2. *Show that* $\mathrm{Nm}_{K/F}(\alpha\beta) = \mathrm{Nm}_{K/F}(\alpha)\mathrm{Nm}_{K/F}(\beta)$ *and* $\mathrm{Nm}_{K/F}(c\alpha) = c^n\mathrm{Nm}_{K/F}(\alpha)$.
3. *Show that* $\mathrm{Nm}_{K/F}(\alpha) = 0$ *iff* $\alpha = 0$.

Problem 3.
1. *For $\alpha = a + b\sqrt{-1} \in \mathbb{C}$ with $a, b \in \mathbb{R}$. Compute* $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha)$ *and* $\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\alpha)$.
2. *Consider $\alpha = \sqrt[3]{2}$ and the field $K = \mathbb{Q}(\alpha) = \left\{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\right\}$. For $x = a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Q}$. Compute* $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ *and* $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$.

The second part was essentially an exam problem last year.

Problem 4. *Given $\alpha \in K$. Show that the minimal polynomial μ_{T_α} of T_α is exactly the minimal polynomial (or minimal irreducible polynomial) of α defined in class, or in Proposition 15.2.3, page 443 of Artin's book.*

Problem 5. *Given $\alpha \in K$. Let $\chi_{T_\alpha} = \det(xI_n - T_\alpha)$ be the characteristic polynomial of α and μ_α be the minimal irreducible polynomial of α.*

(1) *Show that* $\deg \mu_\alpha | n$*;*
(2) *Show that* $\chi_{T_\alpha} = \mu_\alpha^{n/\deg(\mu_\alpha)}$.
(3) *Assume that* $\chi_{T_\alpha} = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ *with* $c_i \in F$. *Find* $\mathrm{Tr}_{K/F}(\alpha)$ *and* $\mathrm{Nm}_{K/F}(\alpha)$ *in terms of* c_i.
(4) *Assume* $\mu_\alpha = x^m + d_{m-1}x^{m-1} + \cdots + d_1 x + d_0$ *with* $d_i \in F$. *Find* $\mathrm{Tr}_{K/F}(\alpha)$ *and* $\mathrm{Nm}_{K/F}(\alpha)$ *in terms of* d_i.
(5) *Show that* $\mathrm{Nm}_{K/F}(\alpha) = (\mathrm{Nm}_{F(\alpha)/F}(\alpha))^{[K:F(\alpha)]}$ *and* $\mathrm{Tr}_{K/F}(\alpha) = [K : F(\alpha)]\mathrm{Tr}_{F(\alpha)/F}(\alpha)$.
(6) *If* $\mathrm{Nm}_{F(\alpha)/F}(\alpha) = 1$. *Show that* $\mathrm{Nm}_{K/F}(\alpha) = 1$.
(7) *If* $\mathrm{Tr}_{F[\alpha]/F}(\alpha) = 0$. *Show that* $\mathrm{Tr}_{K/F}(\alpha) = 0$.

Hint for (2): Use cyclic decomposition.

Problem 6. *Let $p_1, p_2, \ldots, p_n$ are distinct prime integers. Show that the set*

$$\{\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}\}$$

is linearly independent over $\mathbb{Q}$.

This is roughly a problem from Yau College students Math contest, algebra and number theory, 2021, which you can download here. You can also find solutions there. But you are supposed to give a solution based on Trace and Norm you learned from the above problems. The following is a generalization of the above problem but the proof is similar.

Problem 7. *Let $m_1, \ldots, m_k$ be nonzero distinct integers and $n \geq 2$ be a positive integer such that for any two distinct m_i, m_j, the polynomial $x^n - m_i/m_j \in \mathbb{Q}[x]$ is irreducible. Show that the set*

$$\{\sqrt[n]{m_1}, \sqrt[n]{m_2}, \ldots, \sqrt[n]{m_k}\}$$

is linearly independent over $\mathbb{Q}$.

Check that this problem is indeed a generalization of the above one, namely, check that if $p_1, \ldots, p_k$ are distinct primes, then for any two distinct p_i, p_j, the polynomial $x^2 - p_i/p_j \in \mathbb{Q}[x]$ is irreducible. Actually, for any $n \geq 2$, the polynomial $x^n - p_i/p_j \in \mathbb{Q}[x]$ is irreducible. Thus $\{\sqrt[n]{p_1}, \sqrt[n]{p_2}, \ldots, \sqrt[n]{p_k}\}$ is linearly independent over $\mathbb{Q}$.

2. Möbius inversion formula

The following problems are preparations for Ex.7.14, page 474. Consider the set $\mathcal{A} = \{f : \mathbb{Z}_{>0} \to \mathbb{C}\}$, the set of all functions from $\mathbb{Z}_{>0}$ (the set of positive integers) to $\mathbb{C}$. A function $f \in \mathcal{A}$ is called multiplicative if $f(mn) = f(m)f(n)$ for any $m, n \in \mathbb{Z}_{>0}$ with $(m, n) = 1$. For $f, g \in \mathcal{A}$, we define $f * g \in \mathcal{A}$ by

$$f * g(n) = \sum_{d|n} f(d)g(n/d).$$

This is called the Dirichlet product of f with g. Consider the function $I : \mathbb{Z}_{>0} \to \mathbb{C}$ defined by $I(1) = 1$ and $I(n) = 0$ if $n > 1$.

Problem 8. (1) *Show that $f * g = g * f$ and $(f * g) * h = f * (g * h)$ for any $f, g, h \in \mathcal{A}$.*
(2) *Show that $f * I = I * f = f$ for any $f \in \mathcal{A}$.*
(3) *Given $f \in \mathcal{A}$ such that $f(1) \neq 0$. Show that there is a unique function $g \in \mathcal{A}$ such that $f * g = g * f = I$. Find g explicitly. Denote this g by f^{-1}.*

Consider the following function $\mu \in \mathcal{A}$ defined as follows. Suppose $n = p_1^{a_1} \ldots p_k^{a_k}$ is the prime decomposition of n, then define $\mu(n) = 0$ if one of $a_i > 1$. If $a_1 = \cdots = a_k = 1$, define $\mu(n) = (-1)^k$. This function μ is called the Möbius function. Moreover, define $\mu(1) = 1$. Since $\mu(1) \neq 0$, by the above problem, μ has an inverse. It should not be hard to compute it, which is given in the next problem anyway. Define $u : \mathbb{Z}_{>0} \to \mathbb{C}$ by $u(n) = 1$ for any n.

Problem 9. *Show that* $\mu * u = u * \mu = I$.

Using the above problem show that

Problem 10 (Möbius inversion)**.** *Given* $f, g \in \mathcal{A}$. *Show that* $f(n) = \sum_{d|n} g(d), \forall n > 0$ *iff* $g(n) = \sum_{d|n} f(d)\mu(n/d), \forall n > 0$.

All of the above problems are easy. But if it is necessary, the solutions of these problems are given in Section 2 of the book "A classical introduction to modern number theory".

Problem 11. *Let* p *be a prime and let* $q = p^r$ *for some integer* $r \geq 1$. *Let* $M_n(q)$ *be the number of monic irreducible polynomials in* $\mathbb{F}_q[x]$ *of degree* n. *Show that*

$$\sum_{d|n} dM_d(q) = q^n.$$

Moreover, show that $M_n(q) = \frac{1}{n}\sum_{d|n} \mu(d)q^{n/d}$ *using Möbius inversion formula.*

Hint: This is an application of Theorem 15.7.3, (b). More precisely, Theorem 15.7.3, (b) says that

$$x^{p^n} - x = \prod_{d|n}(\text{all monic irreducible polynomials of degree d in } \mathbb{F}_p[x]).$$

A similar equation is true if one replace p by q.

The following is a bonus. For $f \in \mathbb{F}_q[x]$, define $|f| = |\mathbb{F}_q[x]/(f)| = q^{\deg(f)}$. Given a positive integer m, let

$$\pi_q(m) = \#\left\{g \in \mathbb{F}_q[x] : g \text{ monic irreducible, and } |g| \leq m\right\}.$$

Here # denotes the number of elements of a finite set.

Problem 12. *Show that*

$$\lim_{m\to\infty} \frac{\pi_q(m)}{m/\log_q(m)} = 1$$

If you find the analysis involved here is hard, you don't have to do this problem.

Comment: The above is an a prime number theorem for the ring $\mathbb{F}_q[x]$. The prime number theorem for the ring $\mathbb{Z}$ is as follows. Let $\pi(m)$ be the number of all positive prime integers less than m. Then one has

$$\lim_{m\to\infty} \frac{\pi(m)}{m/\ln(m)} = 1.$$

But its proof is much harder.