PROBLEM SET 9

DUE: May 5

Problem 1(**algebraic integers**)

Let $K/\boldsymbol{Q}$ be a finite extension. We say an element $a \in K$ is integral over $\boldsymbol{Q}$ if there exists a monic polynomial $f(x) \in \boldsymbol{Z}[x]$ such that $f(a) = 0$. Let O_K be the set of elements in K integral over $\boldsymbol{Q}$.

(1). Let $\alpha \in K$. Show that the additive group of $\boldsymbol{Z}[\alpha] \subset K$ is finitely generated, if and only if α is integral over $\boldsymbol{Q}$.

(2). Using (1) try to show that $O_K \subset K$ is a subring. (Such a subring is called the ring of algebraic integers of K.)

(3). Let $\mathfrak{m}$ be a maximal ideal of O_K, and let $k = O_K/\mathfrak{m}$ be the residue field. Verify there exists a natural ring epimorphism

$$O_K[x] \to k[x].$$

(4). (**Eisenstein's criterion**) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \in \boldsymbol{Z}[x]$, satisfying

$$a_n \not\equiv 0 \bmod p,\ a_i \equiv 0 \bmod p\ for\ i \neq n,\ a_0 \not\equiv 0 \bmod p^2,$$

where p is a prime. Show that $f(x)$ is irreducible in $\boldsymbol{Z}[x]$.

*(5). What is the ring of algebraic integers of $\boldsymbol{Q}[\sqrt{m}]$ where $m \in \boldsymbol{Z}$ is square-free?

Problem 2(**Gauss lemma**)

Let $f(x), g(x) \in \boldsymbol{Z}[x]$. The **content** of a polynomial is defined to be the greatest common divisors of its coefficients, and denoted by $c(f)$. A polynomial is said to be **primitive** if it has content 1.

(1). Show that $c(fg) = c(f)c(g)$.(Hint: use the morphism in Problem 1).

(2). Then prove that a polynomial is irreducible in $\boldsymbol{Z}[x]$ if and only if it is irreducible in $\boldsymbol{Q}[x]$.

(3). For $K = \boldsymbol{Q}$, show that the product of primitive polynomials is again a primitive polynomial.

Problem 3

(1). Show that the cyclotomic polynomial $f(x) = x^{p-1}+x^{p-2}+....+x+1 \in \boldsymbol{Z}[x]$ is irreducible where p is a prime.

(2). Show that the polynomial $g(x) = 2x^5 - 6x^3 + 9x^2 - 15$ is irreducible in $\boldsymbol{Q}[x]$.

Problem 4

Show that the rings $\boldsymbol{Z}[\sqrt{-1}]$ and $\boldsymbol{Z}[\sqrt{2}]$ are Euclidean rings.

Problem 5

(1). Let K be a field. Show that K contains either $\boldsymbol{Q}$ or $\boldsymbol{F}_p$ as a subfield, where p is a prime. In the former case, K is said to be of characteristic 0, while in the latter case, $char\ K = p$.

(2). Let L/K be a finite extension of fields. Then L can be viewed as a finite dimensional vector space over K. Using this fact show that every finite field has order p^n where p is a prime.

(3). There does not exists a field consisting of 6 elements.

Problem 6

Compute the automorphism groups of the following fields: $\boldsymbol{Q}[\sqrt{2}], \boldsymbol{R}, \boldsymbol{Q}(x)$.

Problem *7

Definition: A **module** M over a ring R is an additive abelian group, together with a scalar product. That is, for any $a, b \in R,\ m, n \in M$, we have

$$a(m+n) = am + an$$

$$(a+b)m = am + bm$$

$$(ab)m = a(bm)$$

$$1m = m$$

We say a set $\{x_i\}_{i \in I}$ is a basis of M if it is linearly independent and generates M. By a free module we shall mean a module which admits a basis, or the zero module.

(1). Prove the following theorem:

Theorem: Let R be a ring and M, N modules over R. Let $\{x_i\}_{i\in I}$ be a basis of M, and $\{y_i\}_{i\in I}$ be a family of elements in N.Then there exists a unique homomorphism $f : M \to N$ with $f(x_i) = y_i$.

(2). Read Section3.7 (Modules over principal rings) of Serge lang's book. Figure it out and use the main theorem to prove the sturcture theorem of finitely generated abelian groups. (If you have enough time).