Lang Chapter 2 (Rings)

0.1 Problem 10

Let D be an integer greater than or equal to 1, and let R be the set consisting of elements in the form $a + b\sqrt{-D}$ where $a, b \in \mathbb{Z}$.

1. *Proof.* We begin by showing that R is indeed a ring under the usual addition and multiplication operations over $\mathbb{C}$. We can see that indeed $r + s = (a_1 + b_1\sqrt{-D}) + (a_2 + b_2\sqrt{-D} = (a_1 + a_2) + (b_1 + b_2)\sqrt{-D}$ for $r, s \in R$. Similarly, $rs = a_1a_2 - b_1b_2D + (a_1b_2 + a_2b_1)\sqrt{-D} \in R$. $\square$

2. *Proof.* We observe that the above observations make R into a subring of $\mathbb{C}$. Thus, there exists an embedding $\phi : R \to \mathbb{C}$ which is a ring homomorphism. Let $\star : \mathbb{C} \to \mathbb{C}$ denote the complex conjugation map. As $\star$ is an automorphism, we can compose the maps $\phi^{-1} \circ \star \circ \phi : R \to R$ to yield an automorphism for R.s $\square$

Problem 11

- Define the ring of trigonometric functions as the polynomial ring $\mathbb{R}[\sin(x), \cos(x)]$.

1. *Proof.* We shall prove that the elements $f(x)$ of the trigonometric polynomial ring R above can be expressed in the following form:

$$f(x) = a_0 + \sum_{m=1}^{n} a_m \sin(mx) + b_m \cos(mx)$$

where $a_m, b_m, a_0 \in \mathbb{R}$.

Every $f \in \mathbb{R}[\sin(x), \cos(x)]$ can be reduced to the form above by associativity and commutivity of the addition and multiplication operations in the field $\mathbb{R}$ and subsequently point-wise multiplication of $\sin(x), \cos(x) \in C(\mathbb{R})$. We invoke the following identities to reduce products of $\sin^m(x), \cos^m(x)$ to products of $\sin(mx), \cos(mx)$:

$$\cos^2(x) = \frac{1 + \cos(2x)}{2}$$

$$\sin^2(x) = \frac{1 - \cos(2x)}{2}$$

We note that by the first and second identities, we can reduce terms of the forms $\cos^{2m}(x), \sin^{2n}(x)$ to the desired forms $(\frac{1+\cos(2x)}{2})^m, (\frac{1-\cos(2x)}{2})^m$ respectively. Futhermore, we have the product-to-sum identities:

$$\sin(x)\sin(y) = \frac{1}{2}[\cos(x-y) - \cos(x+y))]$$
$$\cos(x)\cos(y) = \frac{1}{2}[\cos(x-y) + \cos(x+y))]$$

It is routine verification to see that the combination of the above identities with associativity yields the desired forms for terms $\sin^m(x), \cos^m(x)$. We handle terms of mixed powers of $\sin(x), \cos(x)$ by the similar product-to-sum identity:

$$\sin(x)\cos(y) = \frac{1}{2}[\sin(x-y) + \sin(x-y))]$$

Once again, we inductively reduce the powers of $\sin(x), \cos(x)$ to the forms above then invoke the mixed product-to-sum identity. Combining these reductions, we can inductively reduce the elements of the trigonometric polynomial ring to the desired form, thus concluding the proof.

□

2. *Proof.* We now prove that $\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g)$. Without loss of generality, let $f = a_0 + ... + a_r\cos(rx)$ and $g = b_0 + ... + b_s\cos(sx)$. By multiplying f, g, we yield $fga_0b_0 + .. + a_rb_s\cos(rx)\cos(sx)$. By the product-to-sum identities above, we can reduce this product to the sum

$$a_rb_s\cos(rx)\cos(sx) = \frac{a_rb_s}{2}[\cos((r-s)x) + \cos((r+s)x)]$$

Since $a_r, b_r \neq 0$, $a_rb_r \neq 0$, and $\cos(r+s)x$ is the term with maximum degree by definition above. The equality immidiately follows and we see that R cannot have any zero divisors since the sum of two positive degrees can never be zero. □

Problem 12

• Let P be the set of positive integers. Define the ring R as the set of the functions defined on the set P with values in a commutative ring K with the sum defined to be the pointwise addition of functions and the convolution product to be dictated by the formula

$$(f \star g)(m) = \sum_{xy=m} f(x)g(y)$$

1. *Proof.* We first prove that R is a commutative ring with the unit of R defined to be the function δ which takes $\delta(1) = 1_K$ and $\delta(x) = 0_K$ for $x \neq 1$. To see that R is commutative we note that by the commutativity of K,

$$\sum_{xy=m} f(x)g(y) = \sum_{yx=m} g(y)f(x)$$

By commutativity of P, taking the sum over all factors of m yields

$$\sum_{yx=m} g(y)f(x) = \sum_{xy=m} g(x)f(y) = (g \star f)(m)$$

Let δ be the function as defined above. For $f \in R$.

$$(f \star \delta)(m) = \sum_{xy=m} f(x)\delta(y) = f(m)\delta(1) = f(m)$$

for $m \in P$. As the convolution product agrees with f for all elements in P, δ serves as our unit 1_R. □

2. *Proof.* Suppose we have multiplicative functions $f, g \in R$. Let $m, n \in P$ be relatively prime postive integers. Then:

$$(f \star g)(mn) = \sum_{xy=mn} f(x)g(y)$$

We note that x, y can be decomposed into $x = x_1y_1$ and $y = x_2y_2$ where $x_1x_2 = m$ and $y_1y_2 = n$. Since m, n are relatively prime, it follows that x_1, y_1 and x_2, y_2 are also relatively prime. Hence, we can decompose the product as such

$$\sum_{xy=mn} f(x)g(y) = \sum_{xy=mn} f(x_1)f(y_1)g(x_2)g(y_2) = \sum_{xy=mn} f(x_1)g(x_2)f(y_1)g(y_2) =$$

$$[\sum_{x_1y_1=m} f(x_1)g(y_1)][\sum_{y_1y_2=n} f(y_1)g(y_2)] = (f\star g)(m)(f\star g)(n)$$

Thus, we see that the product is also multiplicative. We see in particular that the set of multiplicative functions endowed with the addition and multiplication operations of R forms a subring of R. □

3. *Proof.* Let μ be the Mobius function defined as follows: $\mu(1) = 1, \mu(p_1...p_r) = (-1)^r$ for $p_1, ..., p_r$ distinct primes, and $\mu(x) = 0$ if $p^2|x$ for some prime p. We first prove that μ is multiplicative. Indeed, let m, n be relatively prime postive integers. We can product mn as a product of distinct prime powers. $\mu(mn) = 0$ if either m, n contains a non-trivial prime power. Thus, it suffices to take the case where mn can be written as a product of single prime powers. Let $m = p_1...p_r$ and $n = p_{r+1}...p_{r+s}$ where all primes are distinct, then $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$. Hence, μ is multiplicative.

   Now consider the convolution product $(\mu * \phi_1)$ where ϕ_1 is the constant function taking values to 1. We can expand the product as follows: Let $m = p_1^{a_1}...p_r^{a_r}$

$$(\mu\star\phi_1)(p_1^{a_1}...p_r^{a_r}) = \sum_{i=1}^{r}\binom{r}{i}(-1)^i$$

   If $m = 1$, then the product is 1 trivially. If $m \neq 1$, then the sum vanishes (proof?). Thus, $(\mu\star\phi_1) = \delta$. □

Problem 15 (Dedekind Rings)

• Let $\mathfrak{o}$ be a subring of field K such that every element of K can be expressed as a quotient of elements of $\mathfrak{o}$
• Define a fractional ideal $\mathfrak{a}$ as a non-zero additive subgroup of K such that $\mathfrak{o}\mathfrak{a} \subseteq \mathfrak{a}$. Since $\mathfrak{o}$ contains the unit element, $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$. Also, we require that there exists a $c \in \mathfrak{a}$ such that $c\mathfrak{a} \subset \mathfrak{o}$. The first property can be interpreted as the "closure of the numerators" i.e for $a\backslash b \in \mathfrak{a}$, $oa\backslash b \in \mathfrak{a}$ for all $o \in \mathfrak{o}$. The second property bounds the denominator to $\mathfrak{o}$.
• A Dedekind ring $\mathfrak{o}$ is ring as above such that its fractional ideals form a group under multiplication with the identity element as $\mathfrak{o}$.

1. We claim that every fractional ideal $\mathfrak{a}$ is finitely generated. Since the set of fractional ideasl under multiplication forms a group, there exists ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$. Thus

there exists $a_1, ..., a_n \in \mathfrak{a}$ and $b_1, ..., b_n \in \mathfrak{b}$ such that:

$$1 = \sum a_i b_i$$

. Hence, for any $a \in \mathfrak{a}$,

$$a = \sum (ab_i) a_i$$