18.781, Fall 2007 Problem Set 10

Solutions to Selected Problems

Problem 1 We have the following identity :

$$sin^2(2\theta) = 4sin^2\theta cos^2\theta = 4sin^2\theta(1 - sin^2\theta)$$

Applying $\theta = \frac{\pi}{12}$ and let $\alpha = sin(\frac{\pi}{12})$. Using $sin\frac{\pi}{6} = \frac{1}{2}$, we have

$$\frac{1}{4} = 4\alpha^2(1 - \alpha^2).$$

That is,

$$16\alpha^4 - 16\alpha^2 + 1 = 0.$$

Therefore, $\alpha = sin(\frac{\pi}{12})$ is algebraic. $\square$

Problem 2 (a) First, let's prove following claim.

There is no element $\alpha \in \mathbb{Z}[\sqrt{-5}]$ such that $N(\alpha) = 2$ or 3.

To prove this, it is enough to show that there is no integral solution (x, y) satisfying $x^2+5y^2 =$ 2 or 3. This is clear.

For $\alpha = 2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$, we have

$$N(2) = 4, N(3) = 9, N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6.$$

Thus for each α, if there is any further factorization $\alpha = \beta\gamma$ with $N(\beta), N(\gamma) > 1$(i.e. each of β, γ is not a unit), since $N(\alpha) = N(\beta)N(\gamma)$, $N(\beta)$ or $N(\gamma)$ should be 2 or 3, which is absurd by the claim.
Hence, 6 is not factorized uniquely, and this implies that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain.

(b) First, we will show that $(3, 1 + \sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 3\}$.

By definition, $(3, 1 + \sqrt{-5}) = \{(r + s\sqrt{-5}) \cdot 3 + (p + q\sqrt{-5}) \cdot (1 + \sqrt{-5}) \mid r, s, p, q \in \mathbb{Z}\} =$ $\{(3r + p - 5q) + (3s + q + p)\sqrt{-5} \mid r, s, p, q \in \mathbb{Z}\}$.

It is clear that $3r+p-5q \equiv 3s+q+p \pmod 3$, so $(3, 1+\sqrt{-5}) \subset \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}, a \equiv b \pmod 3\}$.

For any $a, b \in \mathbb{Z}$ satisfying $a \equiv b \pmod 3$, let $r = \frac{a-b}{3}$ and $p = b$ and $s = q = 0$. Then $(3r+p-5q)+(3s+q+p)\sqrt{5} = a+b\sqrt{-5}$. Hence, $(3, 1+\sqrt{-5}) \supset \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}, a \equiv b \pmod 3\}$, and we proved the claim.

By above observation, it is clear that $(3, 1+\sqrt{-5})$ is not a entire ring $\mathbb{Z}[\sqrt{-5}]$. (For example, $1+2\sqrt{-5}$ is not an element of $(3, 1+\sqrt{-5})$.)

Now we will prove that $(3, 1+\sqrt{-5})$ is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. Let $X = a+b\sqrt{-5}$, $Y = c+d\sqrt{-5}$, and $XY \in (3, 1+\sqrt{-5})$. Then $XY = (ac-5bd)+(ad+bc)\sqrt{-5} \in (3, 1+\sqrt{-5})$, so $(ac-5bd) \equiv (ad+bc) \pmod 3$, and this implies that $(ac+bd) \equiv (ad+bc) \pmod 3$, and $(a-b)(c-d) \equiv 0 \pmod 3$. Thus, $a \equiv b \pmod 3$ or $c \equiv d \pmod 3$, and this is equivalent that X or Y is in $(3, 1+\sqrt{-5})$. Hence $(3, 1+\sqrt{-5})$ is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. $\square$

Problem 3 Let ζ_n be a primitive nth root of unity, and π be a prime element of $\mathbb{Z}[\zeta_n]$ satisfying $\pi \nmid n$.

First let's prove the following claim.

In the ring $R = \mathbb{Z}[\zeta_n]/\pi\mathbb{Z}[\zeta_n]$, $\{1, \zeta_n, {\zeta_n}^2, \cdots, {\zeta_n}^{n-1}\}$ are distinct.

Consider $f(x) = x^n - 1 = (x-1)(x-\zeta_n)\cdots(x-{\zeta_n}^{n-1})$ in R. If some of $\{1, \zeta_n, {\zeta_n}^2, \cdots, {\zeta_n}^{n-1}\}$ are same, namely a, then it is easily verified that $f'(a) = 0$ in R. Note that $f'(x) = nx^{n-1}$. For ${\zeta_n}^i$, assume that $f'({\zeta_n}^i) = n({\zeta_n}^i)^{n-1} = 0$. in R. Since R is an integral domain, $n = 0$ or ${\zeta_n}^{i(n-1)} = 0$ (Which means $\zeta_n = 0$) in R. Since we pick π satisfying $\pi \nmid n$, $n \neq 0$. Also, it is also clear that $\zeta_n \neq 0$ in R, since ζ_n is an unit, so prime element π cannot divide ζ_n. Therefore, there is no ${\zeta_n}^i$ such that $f'({\zeta_n}^i) = 0$, and $\{1, \zeta_n, {\zeta_n}^2, \cdots, {\zeta_n}^{n-1}\}$ are all distinct in R.

Like as the previous problem of problem set 8, this implies that $n \mid N(\pi) - 1$. Now we can define the nth power residue symbol as following:

$$\left(\frac{\alpha}{\pi}\right)_n = \alpha^{\frac{N(\pi)-1}{n}}$$

in the ring R. $\square$

Problem 4

$$\sum_{p:\text{prime}} \frac{1}{p(p-1)} \leqslant \sum_{n=2}^{\infty} \frac{1}{n(n-1)} \leqslant \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) < 1.$$

$\square$

Problem 5

Since h is a primitive root, there is an integer k such that $g = h^k$. Then, $n \equiv g^{v_g(n)} = h^{kv_g(n)} \pmod{q}$. Hence, $v_h(n) = kv_g(n)$. Now define $\zeta' = \zeta^k$. This satisfies $(\zeta')^{q-1} = 1$ clearly, and

$$\zeta^{v_h(n)} = \zeta^{kv_g(n)} = (\zeta')^{v_g(n)},$$

as desired. $\square$

If you have any question, please contact me : Yoonsuk Hyun (yshyun@math.mit.edu)