Math 129 Problem Set 2

Lev Kruglyak

February 7, 2022

Problem 1.21. Show that every element of $\mathbb{Q}[\omega]$ is uniquely expressible in the form

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2}, \quad a_i \in \mathbb{Q} \ \ \forall i$$

by showing showing that ω is the root of the polynomial

$$f(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$$

and that $f(t)$ is irreducible over $\mathbb{Q}$.

Clearly ω is a root of $f(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$ since $t^p - 1 = (t-1)f(t)$ and $\omega \neq 1$. So using the substitution $\omega^{p-1} = -(\omega^{p-2} + \cdots + \omega + 1)$, for any $\alpha \in \mathbb{Q}[\omega]$ we can reduce any $a_0' + a_1'\omega + \cdots + a_n'\omega^n$ to get an expression:

$$\alpha = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2}, \quad a_i \in \mathbb{Q} \ \ \forall i.$$

To prove that this expression is unique, we first must show that $f(t)$ is irreducible in $\mathbb{Z}[t]$. Note that

$$f(t+1) = \frac{(t+1)^p - 1}{t} = \binom{p}{p}x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}.$$

Then $p \mid \binom{p}{k}$ for all $2 \leq k \leq p-1$, $p \nmid \binom{p}{p} = 1$, and $p^2 \nmid \binom{p}{1} = p$. Thus Eisenstein's criterion implies that $f(t+1)$ and hence $f(t)$ is irreducible. Now to prove uniqueness, suppose we had

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} = b_0 + b_1\omega + b_2\omega^2 + \cdots + b_{p-2}\omega^{p-2}.$$

Assuming for the sake of contradiction that $a_i \neq b_i$ for some i, then $(a_0 - b_0) + (a_1 - b_1)\omega + \cdots + (a_{p-2} - b_{p-2})\omega^{p-2} = 0$, so ω is a root of an at most $p-2$ degree polynomial. But ω is the root of f which is minimal because it is an irreducible polynomial of degree $p-1$, so we have a contradiction. Thus $a_i = b_i$ for all i and the expression is unique.

Problem 1.22. Use Problem 1.21 to show that if $\alpha \in \mathbb{Z}[\omega]$ and $p \mid \alpha$, then (writing $\alpha = a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$, $a_i \in \mathbb{Z}$) all a_i are divisible by p. Define congruence mod p for $\beta, \gamma \in \mathbb{Z}[\omega]$ as follows:

$$\beta \equiv \gamma \mod p \quad \Leftrightarrow \quad \beta - \gamma = \delta p, \ \delta \in \mathbb{Z}[\omega].$$

(Equivalently, this is congruence mod the principal ideal $p\mathbb{Z}[\omega]$.)

Suppose $\alpha = p\beta$ for some $\beta \in \mathbb{Z}[\omega]$. Then

$$\alpha = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{p-2}\omega^{p-2} = pb_0 + pb_1\omega + pb_2\omega^2 + \cdots + pb_{p-2}\omega^{p-2} = p\beta$$

for some integers a_i, b_i. By Problem 1.21, these expressions must be equal at a coefficient level, so $a_i = pb_i$ for all i. Thus $p \mid a_i$ for all i.

Problem 1.23. Show that if $\beta \equiv \gamma \mod p$, then $\overline{\beta} \equiv \overline{\gamma} \mod p$, where the bar denotes complex conjugation.

First, note that if $\beta = \beta_0 + \beta_1\omega + \beta_2\omega^2 + \cdots + \beta_{p-2}\omega^{p-2}$, we have

$$\begin{aligned}\overline{\beta} &= \beta_0 + \beta_1\overline{\omega} + \beta_2\overline{\omega^2} + \cdots + \beta_{p-2}\overline{\omega^{p-2}} \\ &= \beta_0 + \beta_1\omega^{p-1} + \beta_2\omega^{p-2} + \cdots + \beta_{p-2}\omega^2 \\ &= \beta_0 + \beta_1(-\omega^{p-2} - \omega^{p-3} + \cdots - \omega - 1) + \beta_2\omega^{p-2} + \cdots + \beta_{p-2}\omega^2 \\ &= (\beta_0 - \beta_1) - \beta_1\omega + (\beta_2 - \beta_1)\omega^{p-2} + \cdots + (\beta_{p-2} - \beta_1)\omega^2.\end{aligned}$$

Now since $\beta \equiv \gamma \mod p$, it follows from Problem 1.22 that $\beta_i \equiv \gamma_i \mod p$. This implies that $\overline{\beta} \equiv \overline{\gamma} \mod p$ by the above expression, since $\beta_i - \beta_1 \equiv \gamma_i - \gamma_1 \mod p$ for $i \neq 1$ and $\beta_1 \equiv \gamma_1 \mod p$.

Problem 1.24. Show that $(\beta+\gamma)^p \equiv \beta^p + \gamma^p \mod p$, and generalize this to arbitrary numbers of terms by induction.

By the binomial theorem,

$$(\beta + \gamma)^p = \sum_{k=0}^{p} \binom{p}{k} \beta^k \gamma^{p-k} \equiv \beta^p + \gamma^p \mod p.$$

because of the basic fact about binomial coefficients which says that $p \mid \binom{p}{k}$ if and only if $1 \geq k \leq p - 1$. The induction argument easily follows from this, giving us the more general claim that $(\beta_1 + \cdots + \beta_n)^p \equiv \beta_1^p + \cdots + \beta_n^p \mod p$.

Problem 1.25. Show that $\forall \alpha \in \mathbb{Z}[\omega]$, α^p is congruent mod p to some $a \in \mathbb{Z}$.

Using Problem 1.21, write $\alpha = a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$. Then by Problem 1.24,

$$\alpha^p = (a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2})^p \equiv a_0^p + a_1^p\omega^p + \cdots + a_{p-2}^p\omega^{p(p-2)} \equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \mod p.$$

Clearly $a_0^p + a_1^p + \cdots + a_{p-2}^p \in \mathbb{Z}$, so we are done.

Problem 2.12. Now we can prove Kummer's lemma on units in the pth cyclotomic field, as stated before Problem 1.26: Let $\omega = e^{2\pi i/p}$, p an odd prime, and suppose u is a unit in $\mathbb{Z}[\omega]$.

1. Show that $u/\overline{u}$ is a root of 1. Use Problem 2.11(c) and observe that complex conjugation is a member of the Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$. Conclude that $u/\overline{u} = \pm\omega k$ for some k.
2. Show that the $+$ sign holds: Assuming $u/\overline{u} = -\omega^k$, we have $u^p = -\overline{u^p}$; show that this implies that u^p is divisible by p in $\mathbb{Z}[\omega]$. But this is impossible because u is a unit.

(a) Note that $\overline{\omega} = \omega^{-1}$, so complex conjugation is a member of $\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$. However $\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong \mathbb{Z}_p^\times$, which is an abelian group so conjugation commutes with any automorphism. So for any $\sigma \in \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$, we have

$$|\sigma(u/\overline{u})| = \left|\sigma(u)/\overline{\sigma(u)}\right| = |\sigma(u)| \,/\, |\sigma(u)| = 1.$$

Thus all of the Galois conjugates of $u/\overline{u}$ have norm 1. It follows from Problem 2.11(c) that $u/\overline{u}$ is a root of unity. By Corollary 2.3, the only roots of unity in $\mathbb{Z}[\omega]$ are $2p$-th roots of unity, so $u/\overline{u} = \pm\omega^k$ for some $k \in \mathbb{Z}$.

(b) Now assume that $u/\overline{u} = -\omega^k$, so $u^p = -\overline{u^p}$. By Problem 1.23, we know that $u^p \equiv \overline{u^p}$, so $2u^p \equiv 0 \mod p$. Since p is an odd prime, we can divide both sides by 2 to get $u^p \equiv 0 \mod p$. This means that $u^p = p\alpha$ for some $\alpha \in \mathbb{Z}[\omega]$, a contradiction because u^p is a unit.

Problem 2.13. Show that 1 and -1 are the only units in the ring $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$, m squarefree, $m < 0, m \neq -1, -3$. What if $m = -1$ or -3?

By Corollary 2 to Theorem 1 we know that for squarefree m,

$$\mathbb{A} \cap \mathbb{Q}[\sqrt{m}] = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2,3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \mod 4 \end{cases}.$$

If $m \equiv 2,3 \mod 4$, then a unit in $A \cap \mathbb{Q}[\sqrt{m}]$ is some $a + b\sqrt{m}$ with $a^2 - mb^2 = 1$, Since a^2 and $-mb^2$ are both nonnegative and $m \neq -1$, the only $a + b\sqrt{m}$ which are units are are $a = \pm 1$. If $m \equiv 1 \mod 4$, then a unit in $A \cap \mathbb{Q}[\sqrt{m}]$ is some $\frac{a+b\sqrt{m}}{2}$ with $a^2 - mb^2 = 4$. Then since a^2 and $-mb^2$ are both nonnegative and $m \neq -3$, the only solution to this are $a = \pm 1$.

Now if $m = -1$, then units satisfy $a^2 + b^2 = 1$ so the only units are $\pm 1, \pm i$. If $m = -3$, then units satisfy $a^2 + 3b^2 = 4$, so the only units are $\pm 1, \frac{1\pm\sqrt{-3}}{2}, \frac{-1\pm\sqrt{-3}}{2}$.

Problem 2.14. Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$, but not a root of 1. Use the powers of $1 + \sqrt{2}$ to generate infinitely many solutions to the Diophantine equation $a - 2b^2 = \pm 1$.

Clearly $1 + \sqrt{2}$ is a unit because $\mathcal{N}(1 + \sqrt{2}) = -1$. Now suppose $a + b\sqrt{2}$ is a unit. Then $(a + b\sqrt{2})(1 + \sqrt{2}) = (a + 2b) + (a + b)\sqrt{2}$ is also a unit. This gives a way to generate infinitely many solutions to $a^2 - 2b^2 = \pm 1$, i.e. given a solution (a, b), there is a larger solution $(a + 2b, a + b)$.

Problem 2.15.

(a) Show that $\mathbb{Z}[\sqrt{-5}]$ contains no elements whose norm is 2 or 3.

(b) Verify that $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is an example of non unique factorization in the ring $\mathbb{Z}[\sqrt{-5}]$.

(a) Suppose $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ has norm 2 or 3. Then $a^2 + 5b^2 = 2, 3$, which is clearly impossible since the smallest value of $a^2 + 5b^2$ which is greater than 1 is $2^2 + 5 \cdot 0^2 = 4$.

(b) Since there is no element of norm 2 or 3, 2 and 3 are irreducible in $\mathbb{Z}[\sqrt{-5}]$. (Any non unit and non zero $a \in \mathbb{Z}$ is irreducible in $\mathbb{Z}[\sqrt{m}]$ if and only if $a = \mathcal{N}(\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{m}]$.) Similarly, $1 \pm \sqrt{-5}$ is irreducible because $\mathcal{N}(1 \pm \sqrt{-5}) = 6$, so any factorization $\alpha\beta = 1 \pm \sqrt{-5}$ would have $\mathcal{N}(\alpha) = 2$ and $\mathcal{N}(\beta) = 3$, however (a) implies that no such elements exist. So $2 \cdot 3$ and $(1 + \sqrt{-5})(1 - \sqrt{-5})$ are two distinct irreducible factorizations of 6.

Problem 2.17. Here is another interpretation of the trace and norm: Let $K \subset L$ and fix $\alpha \in L$; multiplication by α gives a linear mapping of L to itself, considering L as a K-vector space. Let A denote the matrix of this mapping with respect to the basis $\{\alpha_1, \alpha_2, \ldots\}$ for L over K. (Thus the jth column of A consists of the coordinates of $\alpha\alpha_j$ with respect to the α_i.) Show that $T_K^L(\alpha)$ and $N_K^L(\alpha)$ are the trace and determinant of this matrix.

Suppose L has degree n over K, and α has degree d. Let $\{\beta_1, \beta_2, \ldots, \beta_c\}$ be a basis for L over $K[\alpha]$ where $c = n/d$. The basis for L over K can then be written as

$$B = \{\beta_1, \alpha\beta_1, \ldots, \alpha^{d-1}\beta_1, \ldots \beta_c, \alpha\beta_c, \ldots, \alpha^{d-1}\beta_c\}.$$

Now let's consider what multiplication by α does to this basis. If $\alpha^d + a_{d-1}\alpha^{d-1} + a_{d-2}\alpha^{d-2} + \cdots + a_1\alpha + a_0$, then

$$\alpha \cdot \alpha^k \beta_i = \begin{cases} \alpha^{k+1}\beta_i & \text{if } k < d-1 \\ -a_0\beta_i - a_1\alpha\beta_i - \cdots - a_{d-1}\alpha^{d-1}\beta_i & \text{if } k = d-1 \end{cases}.$$

This gives us a matrix of the form:

$$M_B(\alpha) = \begin{bmatrix} M_0 & 0 & \cdots & 0 \\ 0 & M_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_c \end{bmatrix}, \text{ where } M_j = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{d-1} \end{bmatrix}$$

Observe that $\operatorname{tr}(M_B(\alpha)) = -\frac{n}{d}c_{d-1}$, and $\det(M_B(\alpha)) = ((-1)^n c_0)^{n/d}$. By Vieta's theorem and Theorem 2.4', these are exactly equal to $T_K^L(\alpha)$ and $N_K^L(\alpha)$ respectively.

Problem 2.24. Let G be a free abelian group of rank n and let H be a subgroup. Without loss of generality we take $G = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n times). We will show by induction that H is a free abelian group of rank $\leq n$. First we prove it for $n = 1$. Then, assuming the result holds for $n - 1$, let $\pi : G \to \mathbb{Z}$ denote the obvious projection of G onto the first factor (so that an n-tuple of integers gets sent to its first component). Let K denote the kernel of π.

1. Show that $H \cap K$ is a free abelian group of rank $\leq n - 1$.
2. The image $\pi(H) \subset \mathbb{Z}$ is either $\{0\}$ or infinite cyclic. If it is $\{0\}$, then $H = H \cap K$; otherwise fix $h \in H$ such that $\pi(h)$ generates $\pi(H)$ and show that H is the direct sum of its subgroups $\mathbb{Z}h$ and $H \cap K$.

(a) Since $K = \{0\} \oplus \mathbb{Z}^{\oplus n-1}$ is a free abelian group of rank $n - 1$, and $H \cap K$ is a subgroup of K, the inductive assumption implies that $H \cap K$ is a free abelian subgroup of K.

(b) If $\pi(H) = \{0\}$ we are done so suppose $\pi(H)$ is infinite cyclic, generated by $\pi(h)$ for some $h \in H$ (assume without loss of generality that the other components of h are zero). To prove that $H = (H \cap K) \oplus h\mathbb{Z}$, we first need to show that the two subspaces have trivial intersection. Suppose $ah \in H \cap K$ for some $a \in \mathbb{Z}$. This means that $\pi(ah) = 0$, so $\pi(h) = 0$, which is a contradiction unless $a = 0$. Thus 0 is the only element of $(H \cap K) \cap h\mathbb{Z}$.

Next, we must show that every element of H can be expressed as a sum of elements in $H \cap K$ and $h\mathbb{Z}$. Let $g \in H$. Then $g = (g - \pi(g)) + ah$, where $\pi(g) = \pi(ah)$.