HOMEWORK 13

Q2. A complex number is said to be an *algebraic number* if it is algebraic over $\mathbb{Q}$ and an *algebraic integer* if it is the root of a monic polynomial in $\mathbb{Z}[x]$. (Note. A monic polynomial has leading coefficient 1)

(d) If $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$. (Gauss Lemma)

Proof. Let $r = \frac{b}{a}$ $\forall a \in \mathbb{N}, b \in \mathbb{Z}$, where $\gcd(a,b) = 1$. Suppose $f(r) = 0$ for $f \in \mathbb{Z}[x]$ with leading coefficient 1, then $f(x) = g_1(x)g_2(x)\cdots g_k(x)$, where $g_i(x)$ are irreducible with leading coefficient 1. Since $f(\frac{b}{a}) = 0$, $ax - b$ is a factor of $f(x)$, then $\exists g_i(x) = \pm(ax-b)$. Hence $a = 1$ and thus $r = b \in \mathbb{Z}$. $\square$

(e) If u is an algebraic integer and $n \in \mathbb{Z}$, then $u + n$ and nu are algebraic integers.

Proof. Since u is an algebraic integer, there exists $f(x) \in \mathbb{Z}[x]$ such that $f(u) = 0$ with leading coefficient 1. Consider $g(x) = f(x-n)$. $g(x) \in \mathbb{Z}[x]$ and $g(u+n) = f((u+n)-n) = f(u) = 0$ with leading coefficient 1. Thus $u + n$ is an algebraic integer. Next consider $h(x) = n^k \cdot f(\frac{x}{n})$ where $k = \deg f$ and $n \neq 0$. $h(x) \in \mathbb{Z}[x]$ and $h(nu) = n^k f(\frac{nu}{n}) = n^k f(u) = 0$ with leading coefficient 1. Thus nu is an algebraic integer. If $n = 0$, $nu = 0$ is an algebraic integer clearly. $\square$

(f) The sum and product of two algebraic integers are algebraic integers.

Proof. Let $\mathbb{Z}[\alpha,\beta] := \{f(\alpha,\beta) \mid f(x,y) \in \mathbb{Z}[x,y]\}$. It suffices to show $\gamma \in \mathbb{Z}[\alpha,\beta]$ is an algebraic integer. Suppose $\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$ and $\beta^m + b_1\beta^{m-1} + \cdots + b_{m-1}\beta + b_m = 0$ for some $a_i, b_j \in \mathbb{Z}$. Then $\alpha^n = -a_1\alpha^{n-1} - a_2\alpha^{n-2} - \cdots - a_n$ and $\beta^m = -b_1\beta^{m-1} - b_2\beta^{m-2} - \cdots - b_m$. Hence $\mathbb{Z}[\alpha,\beta] = \{\sum_{i<n,j<m} c_{ij}\alpha^i\beta^j \mid c_{ij} \in \mathbb{Z}\}$. Note that $\gamma\alpha^k\beta^\ell \in \mathbb{Z}[\alpha,\beta]$. Hence $\gamma\alpha^k\beta^\ell = \sum_{i<n,j<m} c_{ij}^{k\ell}\alpha^i\beta^j$, i.e.,

$$\gamma\alpha^k\beta^\ell - \sum_{i<n,j<m} c_{ij}^{k\ell}\alpha^i\beta^j = 0 \tag{$\star$}$$

Ordering $\alpha^i\beta^j$ by $\alpha^0\beta^0, \alpha^1\beta^0, \cdots, \alpha^{n-1}\beta^0, \alpha^0\beta^1, \cdots, \alpha^{n-1}\beta^{m-1}$, then ($\star$) becomes $\begin{bmatrix} \gamma - c_{00}^{00} & -c_{10}^{00} & \cdots \\ -c_{00}^{10} & \gamma - c_{10}^{10} & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} \alpha^0\beta^0 \\ \alpha^1\beta^0 \\ \vdots \end{bmatrix} = 0$. Since the matrix is singular, it has determinant 0, i.e., γ is the eigenvalue of $\begin{bmatrix} -c_{00}^{00} & -c_{10}^{00} & \cdots \\ -c_{00}^{10} & -c_{10}^{10} & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}$. Note the characteristic polynomial of a matrix over $\mathbb{Z}$ is monic. Hence γ is an algebraic integer. $\square$

Example 0.1. $n = 2 = m$,

$$\begin{aligned}
(\gamma - c_{00}^{00})\alpha^0\beta^0 - c_{10}^{00}\alpha^1\beta^0 - c_{01}^{00}\alpha^0\beta^1 - c_{11}^{00}\alpha^1\beta^1 &= 0 && ((k,\ell) = (0,0)) \\
-c_{00}^{10}\alpha^0\beta^0 + (\gamma - c_{10}^{10})\alpha^1\beta^0 - c_{01}^{10}\alpha^0\beta^1 - c_{11}^{10}\alpha^1\beta^1 &= 0 && ((k,\ell) = (1,0)) \\
-c_{00}^{01}\alpha^0\beta^0 - c_{10}^{01}\alpha^1\beta^0 + (\gamma - c_{01}^{01})\alpha^0\beta^1 - c_{11}^{01}\alpha^1\beta^1 &= 0 && ((k,\ell) = (0,1)) \\
-c_{00}^{11}\alpha^0\beta^0 - c_{10}^{11}\alpha^1\beta^0 - c_{01}^{11}\alpha^0\beta^1 + (\gamma - c_{11}^{11})\alpha^1\beta^1 &= 0 && ((k,\ell) = (1,1))
\end{aligned}$$

Q3. Let G be an abelian group of order n. A *partial difference set* of G is a subset S of G such that the set $\{x - y \mid x, y \in S, x \neq y\}$ contains $|S| \times (|S| - 1)$ elements.

(a) Let S be a partial difference set of G with $|S| = s$. Then $s^2 - s + 1 \leq n$.

Proof. $s(s-1) \leq n - 1 \Rightarrow s^2 - s \leq n - 1 \Rightarrow s^2 - s + 1 \leq n$. $\square$

(b) Let $a \in U_p$, the set of units of $\mathbb{Z}_p$, be a multiplication generator. Then $S = \{(i, a^i) \mid 0 \leq i \leq p - 1\}$ is a partial difference set of $\mathbb{Z}_p \times \mathbb{Z}_p$. (Hint. Find the desired set of $p(p-1)$ elements)

Sol. There is something wrong with the statement of the problem. For example when $p = 2 \Rightarrow a = 1, S = \{(0,1), (1,1)\}$. Then $(0,1) - (1,1) = (1,0) = (1,1) - (0,1)$, S is not a partial difference set. S might be a partial difference set of $\mathbb{Z}_{p+1} \times \mathbb{Z}_p$.

(c) Let S be as in (b). Then $|(u + S) \cap (v + S)| \leq 1$ for any distinct elements $u, v \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. Suppose not, there exist $(a,b) \neq (c,d) \in (u + S) \cap (v + S)$. Let $(a,b) = u + s = v + s'$ and $(c,d) = u + t = v + t'$ for some $s, s', t, t' \in S$. Then $s - s' = v - u = t - t'$. Hence $s - s' = t - t' \Rightarrow s = t, s' = t' \Rightarrow (a,b) = (c,d)$, a contradiction. $\square$

(d) The statement of this problem is false.