Answers to HW8

1. Tile the plane $\mathbb{C}$ with equilateral triangles starting with the one wwith the vertices $0, 1, j$. This is the ring $\mathbb{Z}[j] = \{a+bj \mid a, b \in \mathbb{Z}\}$. The norm $(a+bj)(a+b\bar{j}) = a^2+ab(j+\bar{j})+j\bar{j}b^2 = a^2+ab+b^2$ takes integer values including $0, 1$, and is multiplicative. To prove it's Euclidean, it remains to show that for every $z, w \neq 0$ there exists t, r (all in $\mathbb{Z}[j]$) such that $z = tw + r$ and $|r| < |w|$, or equivalently, $|z/w - t| < 1$. But z/w falls into one of the tiling equilateral triangles with sidelength 1. So, taking for t one of the vetices of that triangle will do. The units $|u|$ must have the minimal norm $|u| = 1$, i.e. are all the 6th roots of unity $\{j^k \mid k = 0, 1, 2, 3, 4, 5\}$.

In $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$, the multiplicative norm $a^2 + 5b^2$ takes integer values $0, 1, 4, 5, 6, ...$ but misses 2 and 3. Thus, $2 \times 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$ are two factorizations of 6 into irreducibles. This non-uniqueness shows that the ring is not a UFD, hence not a PID, and so cannot be Euclidean. Yet, for u, to be a unit, $|u|^2$ must be invertible within the values of the norm. Thus $|u| = 1$, i.e. $u = \pm 1$ only.

2. Reducible *monic* quadratic polynomilas $x^2 + ax + b$ in $\mathbb{Z}_p[x]$ have the form $(x - \alpha)(x - \beta)$, where $\alpha, \beta \in \mathbb{Z}_p$. The total number of such polinomials is $p(p-1)/2 + (p-1)$ (when $\alpha \neq \beta$ plus when $\alpha = \beta$, i.e. $(p^2 - 1)/2$. This is smaller than the total number p^2 of monic quadratic polinomials. Thus, irrducible $x^2 + ax + b$ exist. Then $F := \mathbb{Z}_p[x](x^2+ax+b)$ is a field of characteristic p with the basis $\hat{1}, \hat{x}$ (cosets of 1 and x) over $\mathbb{Z}_p$, $\hat{x}^2 = -a\hat{x}-b\hat{1}$ is their linear combination. Thus the dimension of F as a vectro space over $\mathbb{Z}_p$ equals 2, and hence $|F| = p^2$.

3. A reducible cubic polynomial $x^3 + ax^2 + bx + c$ will have a root in the field, i.e. $x = 0$ or 1 in $\mathbb{Z}_2$. The root $x = 0$ corresponds to $c = 0$, and $x = 1$ corresponds to $1 + a + b + c = 0$. There are two $(2^3 - 2^2 - 2^2 + 2)$ polynomilas *not* satiafying any of these conditions: $x^3 + x + 1$ and $x^3 + x^2 + 1$. The quotient fields $F_1 := \mathbb{Z}_2[x]/(x^3 + x + 1)$ and $F_2 := \mathbb{Z}_2[y]/(y^3 + y^2 + 1)$ are actually isomorphic. Namely, in F_1, the class $\hat{x}$ is invertible, and hence with the inverse satisfying

$$\left(\frac{1}{\hat{x}}\right)^3 + \left(\frac{1}{\hat{x}}\right)^2 + 1 = \left(\frac{1}{\hat{x}}\right)^3 (1 + \hat{x} + \hat{x}^3) = 0.$$

Thus, the map $\hat{y} \mapsto 1/\hat{x}$ induces an isomorphism $F_2 \to F_1$ between these two fields (of 2^3 elements each).

4. In an $n \times n$ determinant, adding a multiple of one columns to a another does not change the determinant's value. Thus, subtracting the column i from the column j in

$$\Delta(x_1, \ldots, x_n) := \begin{vmatrix} \ldots & 1 & \ldots & 1 & \ldots \\ \ldots & x_i & \ldots & x_j & \ldots \\ \ldots & x_i^2 & \ldots & x_j^2 & \ldots \\ & \ldots & & \ldots & \\ \ldots & x_i^{n-1} & \ldots & x_j^{n-1} & \ldots \end{vmatrix}$$

creates a column with the entries $x_j^k - x_i^k$ all divisible by $x_j - x_i$. Thus, Δ is divisible by $x_j - x_i$. Now, the ring $\mathbb{Z}[x_1, \ldots, x_n]$ is a U.F.D., and $x_i - x_j$ are clearly irreducible in it. Therefore Δ is divisible by $\prod_{j>i}(x_j - x_i)$. The degree of the polynomials are $0+1+2+\cdots+(n-1) = n(n-1)/2$ and $\binom{n}{2}$, i.e. the same. It remains to check the normalization coefficient. In *Delta*, the monomial $x_1^0 x_2^1 x_3^2 \cdots x_n^{n-1}$ occurs with coefficient 1 (it is the product $a_{11}a_{22}\cdots a_{nn}$ of the diagonal entries). In $\prod_{j>i}(x_j - x_i)$, written as the unreduced sum of $2^{n(n-1)/2}$ monomials with coefficients ± 1, the aforementioned product can occur only when the term $+x_j$ is taken from $x_j - x_i$ with $j > i$: there are $n-1$ such x_n, $n-2$ such x_{n-1}, etc. Thus, the coefficient for this term is also 1, and so the polynomials are both non-zero and coincide.