Homework

due on Monday, October 22

Read sections 2.3.1-2.3.3 in Cameron's book and sections 3.5-3.5.4 in Lauritzen's book. Solve the following problems:

Problem 1. Consider the ring $R = \mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$ of Eisenstein integers, where $\omega = (-1+\sqrt{-3})/2$ (see Homework 17 for a proof that this is a ring). Recall that $\omega^2+\omega+1 = 0$. Let $\overline{\omega} = (-1-\sqrt{-3})/2$.

a) Prove that $\overline{\omega}^2+\overline{\omega}+1 = 0$, $\omega\overline{\omega} = 1$, $\overline{\omega} = \omega^2$, $\omega^3 = 1 = \overline{\omega}^3$.

b) Define a map $f : R \longrightarrow R$ by $f(a+b\omega) = a+b\overline{\omega}$. Prove that f is an isomorphism.

c) Consider the map $N : R \longrightarrow \mathbb{Z}$ defined by $N(a+b\omega) = a^2-ab+b^2$. Prove that $N(xy) = N(x)N(y)$ for all $x, y \in R$. Prove that $x \in R$ is invertible iff $N(x) = \pm 1$. Prove that if $|N(x)|$ is a prime number then x is irreducible.

d) Prove that the only invertible elements of $\mathbb{Z}[\omega]$ are $1, -1, \omega, -\omega, \overline{\omega}, -\overline{\omega}$.

e) Suppose that p is a prime and $x, y \in R$ are such that $xy \in pR$. Prove that $p|N(x)$ or $p|N(y)$.

f) Let p be an odd prime such that -3 is a quadratic non-residue modulo p. Prove that if a, b are integers such that $p|a^2-ab+b^2$ then $p|a$ and $p|b$. **Hint.** $(2a-b)^2+3b^2 = 4(a^2-ab+b^2)$.

g) Prove that if a, b are integers such that $2|a^2-ab+b^2$ then $2|a$ and $2|b$.

h) Use e), f), g) to conclude that if $p = 2$ or p is an odd prime such that -3 is a quadratic non-residue modulo p then pR is a prime ideal. Conclude that pR is maximal (Hint: R/pR is finite).

i) Suppose now p is an odd prime such that -3 is a quadratic residue modulo p. Prove that pR is not a prime ideal.

Problem 2. Let R be an integral domain and let $a \in R$ be irrreducible but not prime. Prove that if P is a prime ideal of R and $a \in P$ then P is not principal.

Problem 3. Ler $R = \mathbb{Z}[\sqrt{-6}]$.

a) Prove that $\sqrt{-6}$, 2 and 3 are irreducible in R (use the map N defined in problem 3 of homework 22). Prove that $1, -1$ are the only elements invertible in R.

b) Note that $-6 = \sqrt{-6}\sqrt{-6} = (-2) \cdot 3$ and conclude that R is not a UFD.

c) Prove that the ideal $P =< 2, \sqrt{-6} >$ satisfies $P \cdot P = 2R$.

Remark. In particular, $2 \in P \cdot P$. Note however that 2 cannot be written as ab with $a \in P$ and $b \in P$ (since 2 is irreducible). Thus we get an example justifying our answer to v) of Problem 8 from homework 14.

d) Show that P and $1 + P$ are the only cosets of P in R. Conclude that R/P has two elements and is a field. Use problem 2 to show that P is not principal.