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.

Solution: a) It is straightforward from the formula for the roots of a quadratic polynomial that the roots of $x^2 + x + 1$ are ω and $\overline{\omega}$ (alternatively, just do the computation). Note that $(x-1)(x^2+x+1) = x^3 - 1$. Thus $\omega^3 - 1 = 0 = \overline{\omega}^3 - 1$.

Note that $1, \omega, \overline{\omega}$ are the three roots of the polynomial $x^3 - 1$. But if $a^3 = 1$ then $(a^2)^3 = 1$ so ω^2 is also a root of $x^3 - 1$ and hence we must have $\overline{\omega} = \omega^2$ (it can not be 1 or ω). Finally, $\omega\overline{\omega} = \omega\omega^2 = \omega^3 = 1$. (Altenratively, all the equalities can be verified by a simple explicit computation).

b) Clearly $\overline{\omega} \in R$ so f maps R to R. To see that f is a homomorphism note that

$$f((a + b\omega) + (c + d\omega)) = f((a + c) + (b + d)\omega) = (a + c) + (b + d)\overline{\omega} =$$

$$= (a + b\overline{\omega}) + (c + d\overline{\omega}) = f(a + b\omega) + f(c + d\omega)$$

and

$$f((a+b\omega)(c+d\omega)) = f((ac-bd)+(ad+bc-bd)\omega) = (ac-bd)+(ad+bc-bd)\overline{\omega} =$$

$$= (a + b\overline{\omega})(c + d\overline{\omega}) = f(a + b\omega)f(c + d\omega)$$

(alternatively, just note that f is simply the complex conjugation restricted to the set R and use the properties of complex conjugation). Note now that $f(f(z)) = z$ for all $z \in R$, i.e. $f \circ f$ is the identity, so f its own inverse. Thus f is a bijection and therefore an isomorphism.

c) The first statement follows from the simple observation that

$$N(a + b\omega) = a^2 - ab + b^2 = (a + b\omega)(a + b\overline{\omega}) = (a + b\omega)f(a + b\omega)$$

so $N(x) = xf(x)$ for all $x \in R$, where f is the isomorphism from a). In fact, we have

$$N(xy) = xyf(xy) = xyf(x)f(y) = xf(x)yf(y) = N(x)N(y).$$

If $N(x) = \pm 1$ then $xf(x) = \pm 1$ so x is invertible. Conversely, assume that x is invertible. Then $xy = 1$ for some $y \in R$ and therefore

$$1 = N(1) = N(xy) = N(x)N(y).$$

Since both $N(x)$, $N(y)$ are integers, we must have $N(x) = \pm 1$.

Suppose now that $|N(x)|$ is a prime number. If $x = st$ for some $s, t \in R$, then $|N(x)| = |N(st)| = |N(s)||N(t)|$. But $|N(x)|$ is a prime number and $|N(s)|$, $|N(t)|$ are integers, so one of $|N(s)|$, $|N(t)|$ must be equal to 1. By our previous observation, this means that one of s, t is invertible. Thus x is irreducible.

Remark: Note that $N(x)$ is non-negative for all $x \in R$, so the absolute value above is not needed and $N(x) = -1$ is not possible.

d) By c), the element $a+b\omega$ is invertible iff $a^2-ab+b^2 = 1$. Note that $a^2-ab+b^2 = (a-b/2)^2 + 3b^2/4 = 3a^2/4 + (b-a/2)^2$. Since a, b are integers, we see that if $a^2 - ab + b^2 = 1$ then both $|a| < 2$ and $|b| < 2$. Now it is straightforward to see that the only integral solutions to $a^2 - ab + b^2 = 1$ are $(1,0)$, $(-1,0)$, $(0,1)$, $(0,-1)$, $(-1,-1,)$, $(1,1)$. These correspond to $1, -1, \omega, -\omega, \overline{\omega}, -\overline{\omega}$ respectively.

e) If $xy \in pR$ then $xy = pz$ for some $z \in R$. Thus

$$N(x)N(y) = N(xy) = N(pz) = N(p)N(z) = p^2N(z).$$

Since the values of N are integers, we see that $p|N(x)N(y)$. It follows that $p|N(x)$ or $p|N(y)$.

f) Suppose that $p|a^2 - ab + b^2$. Since $(2a-b)^2 + 3b^2 = 4(a^2 - ab + b^2)$, we have $p|(2a-b)^2 + 3b^2$, i.e $(2a-b)^2 \equiv -3b^2 \pmod{p}$. If $p \nmid b$ then multiplying the congruence by b^{p-3} and using Fermat's Little Theorem, we get

$$[(2a-b)b^{(p-3)/2}]^2 \equiv -3b^{p-1} \equiv -3 \pmod{p}$$

which contradicts our assumption that -3 is a quadratic non-residue mudulo p. Thus we must have $p|b$. Since $p|a^2 - ab + b^2$, we have $p|a^2$ so also $p|a$.

g) If both a, b are odd or if one of them is odd and the other even then $a^2 - ab + b^2$ is odd. On the other hand, if both a, b are even then clearly $a^2 - ab + b^2$ is even. This proves the claim.

h) Suppose $xy \in pR$, where $x = a + b\omega$, $y = c + d\omega$. By e), we have $p|N(x)$ or $p|N(y)$. If $p|N(x) = a^2 - ab + b^2$ then by f) and g) we get $p|a$ and $p|b$ so $a + b\omega \in pR$. Similarly, if $p|N(y)$ then $c + d\omega \in pR$. This proves that pR is a prime ideal. Note now that R/pR has p^2 elements so it is a finite domain, hence a field. It follows that pR is maximal.

i) Suppose that -3 is a quadratic residue modulo p, so $k^2 \equiv -3 \pmod{p}$ for some integer k. We may assume that $k = 2l - 1$ is odd (if not, replace k by $p + k$). To show that pR is not prime it suffices to find integers a, b such that $x = a + b\omega$,

$y = a + b\overline{\omega} = a - b - b\omega$ do not belong to pR but $xy = a^2 - ab + b^2$ belongs to pR. This will be the case if $p \nmid b$ but $p|a^2 - ab + b^2$. Let us take $a = l$, $b = 1$ so $a^2 - ab + b^2 = l^2 - l + 1 = [(2l-1)^2 + 3]/4 = (k^2 + 3)/4$. Since p is odd and $p|k^2 + 3$, we see that $p|l^2 - l + 1$. We showed that neither $x = l + \omega$ nor $y = l + \overline{\omega}$ belong to pR but $xy \in pR$. Thus pR is not prime.

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.

Solution: Suppose that a is irreducible but not prime and let P be a prime ideal containing a. Thus $aR \subseteq P$ but $aR \neq P$ (since a is not prime). Recall that a is irreducible iff aR is maximal among all proper principal ideals. Since P is proper and bigger than aR, it can not be principal.

Another argument: Suppose that $P = bR$ is principal. Since P is proper, b is not invertible. Since $a \in P = bR$, we have $a = bc$ for some $c \in R$. But a is irreducible, so either b or c is invertible. We alread know that b is not invertible, so c is invertible and therefore $aR = bR$, a contradiction. It proves that 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.

Solution: a) We will use te map N defined by $N(a + b\sqrt{-6}) = a^2 + 6b^2$. Note that if $b \neq 0$ then $N(a + b\sqrt{-6}) \geq 6$. Recall now that we proved in Problem 3 of homework 22 that $a + b\sqrt{-6}$ is invertible iff $N(a + b\sqrt{-6}) = \pm 1$. Thus $a + b\sqrt{-6}$

is invertible iff $b = 0$ and $a = \pm 1$, which proves that $1, -1$ are the only invertible elements of R.

Observe now that if $a + b\sqrt{-6}$ is not invertible then either $b \neq 0$ or $|a| \geq 2$, so in both cases $N(a + b\sqrt{-6}) \geq 4$ Consequently, if neither x nor y is invertible then $N(xy) = N(x)N(y) \geq 4 \cdot 4 = 16$. In other words, if $z \in R$ is not irreducible then $N(z) \geq 16$. But $N(\sqrt{-6}) = 6$, $N(2) = 4$, $N(3) = 9$, so $2, 3, \sqrt{-6}$ are all irreducible.

b) By a), $-6 = \sqrt{-6}\sqrt{-6} = (-2) \cdot 3$ are two irreducible factorizations of -6. . Since $1, -1$ are the only units of R, neither 2 nor 3 is associated to $\sqrt{-6}$. Thus these factorizations are not equivalent and therefore R is not a UFD.

c) Since $P =< 2, \sqrt{-6} >$, we have (by Problem 3 of homework 19)

$$P \cdot P =< 2 \cdot 2, 2 \cdot \sqrt{-6}, \sqrt{-6} \cdot \sqrt{-6} >=< 4, 2 \cdot \sqrt{-6}, -6 >$$

We see that every generator of $P \cdot P$ belongs to $2R$, so $P \cdot P \subseteq 2R$. On the other hand, $2 = (-1) \cdot 4 + (-1)(-6) \in P \cdot P$ (since both 4 and -6 are in $P \cdot P$), so $2R \subseteq P \cdot P$. This proves that $2R = P \cdot P$.

d) Clearly $1 \notin P$ (otherwise we would have $R = P$ and $P^2 = R$, which contradicts c)) so P and $1 + P$ are different cosets. Now if $x = a + b\sqrt{-6}$ and $a = 2c$ is even then $x = c \cdot 2 + b\sqrt{-6} \in P$, so $x + P = P$. If $x = a + b\sqrt{-6}$ and $a = 2c + 1$ is odd then $x - 1 = c \cdot 2 + b\sqrt{-6} \in P$, so $x + P = 1 + P$. This proves that P and $1 + P$ are the only cosets of P in R. Thus R/P has 2 elements and is isomorpphic to the field $\mathbb{Z}/2$. Thus P is a mximal ideal, so also a prime ideal. Note that $2 \in P$. Recall that 2 is irreducicble. Note however that 2 is not prime since $\sqrt{-6} \notin 2R$ bur $\sqrt{-6}^2 = -6 \in 2R$. By problem 2, P is not principal.