Math 504, Fall 2013
HW 1

1. Let R be the ring of continuous functions $[0,1] \to \mathbb{R}$ with point-wise addition and multiplication. Prove that the set of functions vanishing at a point $x \in [0,1]$ is a maximal ideal in R, we denote it by m_x. If m is a maximal ideal of R that is not equal to m_x for any $x \in [0,1]$, show that there are a finite set of elements $f_1, \dots f_n$ in m that have no common zero on $[0,1]$; by considering $f_0^2 + \cdots + f_n^2$, show that there in no such m; i.e, the maximal ideal in R are the ideal $m_x,\ x \in [0,1]$.

Let e_x be the ring homomorphism $R \to \mathbb{R}, f \mapsto f(x)$. It's surjective since R contains all the constant functions, and by definition $\ker e_x = m_x$. Since $\mathbb{R}$ is a field, it follows that m_x is a maximal ideal of $\mathbb{R}$.

Suppose now M is a maximal ideal different from all the m_x's. In particular, $M \nsubseteq m_x$ for any x, i.e. for any x there is $f_x \in M$ such that $f_x(x) \neq 0$. By continuity, we can assume $f_x \neq 0$ in an open neighborhood U_x of x. Since the U_x's form an open cover of the compact set $[0,1]$, there is a finite subcover $U_1, \dots, U_n$, corresponding to the elements $f_1, \dots, f_n$. Let $g := f_1^2 + \ldots + f_n^2 \in M$. Since the f_i's have no common zeroes, g is never zero, hence invertible in R. This implies that $M = R$, hence every maximal ideal is of the form m_x for some x. ∎

2. Factor $x^8 - 1$ and $x^{12} - 1$ in $\mathbb{Q}[x]$.

$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$
$x^{12} - 1 = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)$
That equality holds above over $\mathbb{Q}$ is just computation, and that $x-1$ and $x+1$ are irreducible over $\mathbb{Q}[x]$ is immediate. What remains is to show the irreducibility of the quadratics and quartics. We note that we are implicitly using the fact quadratics in $\mathbb{Q}[x]$ are reducible if and only if they have linear terms, a fact which follows immediately by the division algorithm. For quartics, they could have a linear factor or be the product of irreducible quadratics. By the rational roots test, the only possible rational roots for all polynomials are ± 1. A computation yields that neither 1 nor -1 are zeros of any of the quadratics, so they are all irreducible in $\mathbb{Q}[x]$. If the quartic $x^4 + 1$ is the product of irreducible quadratics, then $x^4 + 1 = (x^2 + bx + c)(x^2 + dx + e)$ (we can take both leading coefficients to be 1), which furnishes the system of equations

$$\begin{aligned} d + b &= 0 \\ e + c + db &= 0 \\ dc + be &= 0 \\ ec &= 1, \end{aligned}$$

and $d = -b$ implies the third equation becomes $-b(c+e) = 0$. If $c = -e$, then the fourth equation cannot be solved since $-c^2 = 1$ has no solutions in $\mathbb{Q}$. If $b = 0$, then $d = 0$, then the second equation gives $e = -c$ again, which is impossible. Thus $x^4 + 1$ is not the product of quadratics and is hence irreducible over $\mathbb{Q}[x]$. We now seek a representation of $x^4 - x^2 + 1 = (x^2 + bx + c)(x^2 + dx + e)$, which furnishes a similar system of equations

$$\begin{aligned} d + b &= 0 \\ e + c + db &= -1 \\ dc + be &= 0 \\ ec &= 1. \end{aligned}$$

If $d = -b$, the third equation again becomes $-b(c+e) = 0$. If $c = -e$, then the fourth equation cannot be solved since $-c^2 = 1$ has no solutions in $\mathbb{Q}$. If $b = 0$, then $d = 0$ and the second equation reads $e + c = -1$. If $e = c + 1$, then $c(c+1) = 1$ has no solutions over $\mathbb{Q}$ (quadratic formula), so we conclude this quartic is irreducible. ∎

3. If d and e are greatest common divisors of $\{a_1, \ldots a_n\}$ in a domain R, show that d and e are associates, i.e. unit multiples of one another.

Since they are both greatest common divisors, $d \mid e$ and $e \mid d$. Therefore, $e = xd$ and $d = ye$ for some $x, y \in R$. Therefore, $e = xd = x(ye) = (xy)e$ and it follows that $1 = xy$ since R is a domain, hence e and d are associates. ∎

4. Let $k[x,y]$ be the polynomial ring on two variables with coefficients in the field k. Show that the ideal $J = k[x,y]_{\geq n} = \text{span}\{x^i y^j \mid i + j \geq n\}$ can be generated by $n+1$ elements, but not by n elements. (Hint: Think of degree).

First of all, it's clear that J can be generated as an ideal by the $n+1$ monomials $x^n, x^{n-1}y, \ldots, y^n$. We'll show that it can't be generated by less than $n+1$ elements.

Let G be any finite generating set for J, and let G_0 be the set consisting of the degree n part of the polynomials in G. We claim that $J = (G_0)$. Since one containment is clear, it will suffice to show that $x^i y^{n-i} \in (G_0)$ for all $i \leq n$.

Indeed, we know that

$$x^i y^{n-i} = \sum p_j(x,y) g_j(x,y) \quad \text{ with } g_j \in G$$

If we write $p_j(x,y) = p_j(0,0) + p_j'$ and $g_j = \tilde{g}_j + g_j'$ where $\tilde{g}_j$ is the degree n part of g_j. Then the only degree n term in the product $p_j(x,y)g_j(x,y)$ is $p_j(0,0)\tilde{g}_j$, and since in the above sum the terms of degree $> n$ cancel, we have

$$x^i y^{n-i} = \sum p_j(0,0)\tilde{g}_j$$

This shows that the monomials $x^i y^{n-i}$ are in the k span of G_0.

Assume now has at most n elements: then we would have that the k span of G_0, contains an $n+1$-dimensional subspace, impossible.

∎

5. Show that the ring of Gaussian Integers, $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$, is a Euclidean domain with respect to the functions $\delta : Z[i] \to \mathbb{Z}$ defined by $\delta(x) := x\bar{x}$, where $\bar{x}$ denote the complex conjugate of x.

Let $f, g \in \mathbb{Z}[i]$, with $g \neq 0$: we have to define a way to divide f by g. We know that $f/g \in \mathbb{C}$. Since in $\mathbb{C}$ a point can never be further than a distance of $\sqrt{2}/2$ from a lattice point, then there must be $q \in \mathbb{Z}[i]$ at a distance less than or equal to $\sqrt{2}/2$ from f/g. Thus $f/g = q + r_0$ with $|r_0| \leq \sqrt{2}/2$. This implies that $f = qg + r_0 g$ with $r_0 g = f - qg \in \mathbb{Z}[i]$. Call $r_0 g = r$. Then $\delta(r) = \delta(g r_0) = g r_0 \overline{g r_0} = g\bar{g} r_0 \bar{r}_0 = \delta(g)(|r_0|)^2 \leq \delta(g)/2 < \delta(g)$. So $f = qg + r$ with $\delta(r) < \delta(g)$ that is what we wanted to prove.

■

6. Factor 2, 3 and 5 in $\mathbb{Z}[i]$ as products of primes.

We claim that $2 = (1+i)(1-i)$, $3 = 3$, and $5 = (2+i)(2-i)$ are prime factorizations in $\mathbb{Z}[i]$.

First, suppose $1 + i | (a + bi)(c + di)$. But

$$(a + bi)(c + di) = (a - b)(c - d) + (1 + i)(bc + da + (i - 1)bd)$$

so $(1 + i)|(a - b)(c - d)$. This means $(1 + i)(e + if) = (a - b)(c - d)$. Comparing i coefficients, we see $e + f = 0$, so in fact $e(1 + i)(1 - i) = 2e = (a - b)(c - d)$. Suppose without loss of generality that $2|a - b$. Then $(1 + i)|2|a - b$. But $a + bi = a - b + b(1 + i)$ so in fact $1 + i|a + bi$. Hence $1 + i$ is prime. By symmetry, $1 - i$ is prime as well.

To show 3 is prime in $\mathbb{Z}[i]$, suppose $3|(a + bi)(c + di)$. Then $3|(a^2 + b^2)(c^2 + d^2)$ after multiplying by conjugates. So without loss of generality, $3|a^2 + b^2$. In $\mathbb{F}_3$, the only solution to $a^2 + b^2 = 0$ is $a = b = 0$. So $3|a, b$ hence $3|a + bi$. So 3 is prime.

Lastly, $2 + i$ is prime for the same reason $1 + i$ is prime, but we repeat the proof for completeness. Suppose $2 + i|(a + bi)(c + di)$. But

$$(a + bi)(c + di) = (a - 2b)(c - 2d) + (2 + i)(bc + da + (i - 2)bd))$$

so $(2 + i)|(a - 2b)(c - 2d)$. This means $(2 + i)(e + if) = (a - 2b)(c - 2d)$. Comparing i coefficients, we see $e + 2f = 0$, so in fact $e(2 + i)(2 - i) = 5e = (a - 2b)(c - 2d)$. Suppose without loss of generality that $5|a - 2b$. Then $(2 + i)|5|a - 2b$. But $a + bi = a - 2b + b(2 + i)$ so in fact $2 + i|a + bi$. Hence $2 + i$ is prime. By symmetry, $2 - i$ is prime as well.

In conclusion, $2 = (1 + i)(1 - i)$, $3 = 3$, and $5 = (2 + i)(2 - i)$ are the corresponding prime factorizations.

One can also also argue that Euclidean domains are UFDs, so prime is equivalent to irreducible, and use the norm of problem 9 to show that $1 + i, 3$ and $2 + i$ are irreducible.

■

7. Prove that a Euclidean domain is a PID.

Let R be a Euclidean domain with respect to the function $\delta : R \to \mathbb{Z}$. Let $I \subset R$ be an ideal that is not 0. Choose $s \in I$ such that $s \neq 0$ and $\delta(s) = \min\{\delta(r) : r \in I\}$; such an element is guaranteed to exist because $\delta(r) \geq 0$ for all $r \in R$.

Choose any other $r \in I$. By definition, there exists $q_1, q_2 \in R$ such that $r = q_1 s + q_2$ with $q_2 = 0$ or $\delta(q_2) < \delta(s)$. Since I is an ideal, $q_1 s \in I$ and $r - q_1 s = q_2 \in I$. We choose s to be of minimal norm among elements in I, so it must be that $q_2 = 0$. Then for all $r \in I$, there exists $q \in R$ such that $r = sq$. That is, $I \subset (s)$. It's already true that $(s) \subset I$, so $(s) = I$ and I is a principal ideal. R and I were arbitrary, so this shows that every Euclidean domain is a PID. ∎

8. Let $A = k[x, x^{-1}]$ be the subring of $k(x)$ generated by x, x^{-1} and k. Is $k[x, x^{-1}]$ a PID? Why?

Let I be an ideal of A, and let $J := I \cap k[x]$. Then J is an ideal of $k[x]$, hence it's principal, say $J = (p)$. We claim that $I = (p)$ in A, thus showing that every ideal in A is principal.

Clearly, $(p) \subseteq I$. Conversely, let $f \in I$. Then we can write $f = x^n f'(x)$ where $f'(x) \in k[x]$ and $n \in \mathbb{Z}$. Since $f' = x^{-n} f$ is also in I, then $f' \in J$ so f' is a multiple of p in $k[x]$. It follows that f is a multiple of p, so $I = (p)$ as claimed. ∎

9. Let d be a square-free positive integer. Define the norm function $N : \mathbb{Z}[\sqrt{-d}] \to \mathbb{Z}$ given

$$N(a + b\sqrt{-d}) = a^2 + b^2 d^2$$

1. Establish some important properties of N.
2. Show that u is a unit in $\mathbb{Z}[\sqrt{-d}]$ if and only if $N(u) = 1$.
3. Show that the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.
4. If $d > 1$, show that the only units in $\mathbb{Z}[\sqrt{-d}]$ are ± 1.

1. The fundamental property of the norm is that $N(a)N(b) = N(ab)$, as a simple calculation shows. Also, it's clear from the definition that N has values in $\mathbb{N}$.
2. Suppose that u is a unit in $\mathbb{Z}[\sqrt{-d}]$ and let u be its inverse. By part (1) be know that N is multiplicative, so $N(u)N(u^{-1}) = N(1) = 1$. As each of $N(u)$ and $N(u^{-1})$ are in $\mathbb{N}$, both must be 1.

   Conversely, if $N(u) = u\overline{u} = 1$, then since $\overline{u} \in \mathbb{Z}[\sqrt{-d}]$ we have that u is a unit.
3. It's easy to see that the only elements whose norm is 1 are $\pm 1, \pm i$, and by part (2) they are the only units.
4. As above, if $d > 1$ the only elements with norm one are ± 1.

∎

10. Find an element in $R = \mathbb{C}[x,y,z]/(xy - z^2)$ that is irreducible but not prime.

Since in R we have $xy = z^2$, then $x|z^2$. We'll show that x does not divide z, thus implying that x is not prime.

Suppose $z = xp$ in R for some p. Then this means that

$$z = xp + q(xy - z^2) \quad \text{for some } q$$

where this is an equality in $\mathbb{C}[x,y,z]$.

Now write $p = \sum p_i$ and $q = \sum q_i$ as the sum of their homogeneous components. Every term of $q(xy - z^2)$ has degree at least 2, and they have to cancel with the terms of $x(p_1 + p_2 + \ldots)$. It follows that $z = xp_0$, absurd.

We now claim that x is irreducible. First of all, observe that the automorphism $z \mapsto -z$ of $\mathbb{C}[x,y,z]$ descends to an automorphism ϕ of R. Define $N : R \to R$ as $N(p) = p\phi(p)$, much like the norm in problem 9. For any other element in R, note that it can be written uniquely as $p(x,y) + zq(x,y)$, thus $N(p(x,y) + zq(x,y)) = p^2 - xyq^2$. We can then regard N as having values in $\mathbb{C}[x,y]$. As in problem 9, the units are characterized by the fact that their norm is invertible in $\mathbb{C}[x,y]$, and one can check directly that $N(ab) = N(a)N(b)$.

We have that $N(x) = x^2$ and if $x = \alpha\beta$ were not irreducible then $N(x) = N(\alpha)N(\beta)$. If we can prove we can't have $N(\alpha) = x$, then this would force $N(\alpha) = x^2$ so that $N(\beta)$ would be invertible, hence β would be a unit in R.

If $N(\alpha) = x$, then

$$x = p^2 - xyq^2$$

for some polynomials p, q. Since $x|p^2$, then $x|p$ hence we can divide by x to get

$$1 = x(p')^2 - yq^2$$

Evaluating at $x = y = 0$ yields a contradiction.

This means that x is irreducible but not prime.

■