Algebra Homework 4

Gandhar Kulkarni (mmat2304)

October 5, 2023

1

Let $R = \mathbb{Z}[\omega]$.

1. Prove that R is a Euclidean Domain.
2. For any $\alpha = a + b\omega \in R$, set $\tilde{\alpha} := a + b\omega^2$. If π is a prime in R, prove that either π is associate to a prime p in $\mathbb{Z}$ or $|\pi\tilde{\pi}| = p$ for some prime $p \in \mathbb{Z}$. Moreover, every prime p in $\mathbb{Z}$ occurs in one of these two cases.
3. For any prime $p \in \mathbb{Z}$, prove that the following conditions are equivalent:
   (a) p splits in R, i.e., $p = |\pi\tilde{\pi}|$ for some $\alpha \in R$, i.e., $p = a^2 \pm ab + b^2$ for some $a, b \in \mathbb{Z}$.
   (b) $x^2 \pm x + 1$ has a root in $\mathbb{F}_p$, i.e., there exists $a \in \mathbb{F}_p$ such that $a \neq 1$, $a^3 = 1$.
   (c) $p = 3$ or $p \equiv 1(\mod 3)$.
4. Prove that a positive integer n can be written as $n = a^2 \pm ab + b^2$ for $a, b \in \mathbb{Z}$ iff any prime of the form $3k - 1$ occurs in the prime factorisation of n an even number (0 also allowed) of times.
5. Find all ways of writing $2100 = a^2 - ab + b^2$.

Solution:

1. We take $\alpha, \beta \in R$, $\beta \neq 0$. Then we propose that $N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$ is a good choice for the size function. Then $\frac{\alpha}{\beta} \in \mathbb{Q}(\omega)$, and we can write it as $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = q_1 + q_2\omega$. Then we can find $m, n \in \mathbb{Z}$ such that $|q_1 - m| \leq \frac{1}{2}, |q_2 - n| \leq \frac{1}{2}$. Therefore, see that

$$|\frac{\alpha}{\beta} - (m + n\omega)| = |q_1 - m + \sqrt{2}(q_2 - n)| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

   Thus we have $\left|\frac{\alpha}{\beta} - (m + \omega n)\right| < 1 \implies |\alpha - \beta(m + \omega n)| < |\beta|$. Setting $|\alpha - \beta(m + \omega n)| = r$, we have our answer.

2. Let π be a prime in R. Then $\pi\overline{\pi} = p_1 \dots p_k$, where $p_1, \dots, p_k$ are primes in R. Since π and $\overline{\pi}$ are conjugates, and they are primes themselves, k can be at most 2. In the case where $k = 1$, we have the case that $\pi\overline{\pi} = p$. Thus we have $|\pi\overline{\pi}| = p$. In the case where $k = 2$, we have $\pi\overleftarrow{\pi} = p_1p_2$. Let $\pi|p_1$, then we must have $\overline{\pi}|\overline{p_1}$. If $p_1 = \overline{p_1}$, then $p_1 = p_2 = p \in \mathbb{Z}$. If $p_2 = \overline{p_1}$, we can also see that $p_1 = \overline{p_2}$ by the same argument using $\overline{\pi}|p_2$. Then we have $p_1 = p_2 = p \in \mathbb{Z}$. This means that π must be an associate of a prime in $\mathbb{Z}$.

3. (a) (a) $\implies$ (b): We know that there exist $a, b \in \mathbb{Z}$ such that $p = a^2 \pm ab + b^2$. Then $a^2 \pm ab + b^2 \equiv 0 \mod p$. Both a and b must be non-zero, since say if $b = 0$ then $p = a^2$, which is absurd. Then b^{-1} must exist, and we must have $(ab^{-1})^2 \pm (ab^{-1}) + 1 \equiv 0 \mod p$, which means that ab^{-1} is a root for the equation $x^2 \pm x + 1$ in $\mathbb{F}_p[x]$.
   (b) (b) $\implies$ (c): We have a $a \in \mathbb{F}_p$ such that $a^3 = 1$. The multiplicative group of units in $\mathbb{F}_p$ has $p - 1$ elements, and we can see that the cyclic subgroup generated by a is of order 3. This means that $3|p - 1$, which implies that $p \equiv 1 \mod 3$.
   (c) (c) $\implies$ (b): If $p = 3$ then $3 = 1^2 + 1 \cdot 1 + 1^2$. If $p \equiv 1 \mod 3$, then $3|p - 1$. By Cauchy's theorem, there must exist an elements of order 3 in the group of units in $\mathbb{F}_p$. Thus $a \in \mathbb{F}_p^\times$ such that $a \neq 1$ and $a^3 = 1$.

(d) (b) $\implies$ (a): We will prove the contrapositive. Let us say that p does not split in R. Then we have that p is prime in R. Then see that

$$\frac{\mathbb{Z}[\omega]}{(p)} \cong \frac{\mathbb{Z}[x]}{(x^2 \pm x + 1, p)}$$

is a domain. Then

$$\frac{\mathbb{Z}[x]}{(x^2 \pm x + 1, p)} \cong \frac{\mathbb{F}_p[x]}{(x^2 \pm x + 1)}$$

is a domain. Since $\mathbb{F}_p[x]$ is a PID, $(x^2 \pm x + 1)$ which is a prime ideal must now also be irreducible. Therefore there is no root of $x^2 \pm x + 1$ in $\mathbb{F}_p[x]$

4. Let $n = p_1^{a_1} \dots p_r^{a_r} \cdot q_1^{b_1} \dots q_s^{b_s}$ be a prime factorisation of a number $n \in \mathbb{Z}$. All the p_i's are of the form $3k-1$, while the q_j's are either 3 or of the form $3k+1$. Then see that the primes of the second type split and become an expression of the form $a^2 \pm ab + b^2$ while the other primes do not split. Take $p_1^{a_1}$. To factor into the expression $a^2 \pm ab + b^2$, a_1 must be even as the expression is a homogenous form of degree 2. Therefore all primes of the form $3k-1$ should occur even number of times.

5. $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$. 3, and 7 will split while 2 and 5 will remain inert. Since 2 and 5 appear twice, it is possible to write 2100 as $a^2 \pm ab + b^2$ in at least one way. The units in $\mathbb{Z}[\omega]$ are $\pm 1, \pm\omega, \pm\omega^2$. See that $3 = (2+\omega)(2+\omega^2)$ and $7 = (3+\omega)(3+\omega^2)$. We have two choices as to which terms we could multiply with each other. Then, ignoring units, we have 2 possible ways to split 2100.

2

Let $R = \mathbb{Z}[\sqrt{2}]$.

1. Prove that R is a Euclidean Domain.

2. For any $\alpha = a + b\sqrt{2} \in R$, set $\tilde{\alpha} := a - b\sqrt{2}$. If π is a prime in R, prove that either π is associate to a prime p in $\mathbb{Z}$ or $|\pi\tilde{\pi}| = p$ for some prime $p \in \mathbb{Z}$. Moreover, every prime p in $\mathbb{Z}$ occurs in one of these two cases.

3. For any prime $p \in \mathbb{Z}$, prove that the following conditions are equivalent:

   (a) p splits in R, i.e., $p = |\pi\tilde{\pi}|$ for some $\alpha \in R$, i.e., $p = |a^2 - 2b^2|$ for some $a, b \in \mathbb{Z}$.

   (b) $x^2 - 2$ has a root in $\mathbb{F}_p$, i.e., there exists $a \in \mathbb{F}_p$ such that $a^2 = 2$.

   (c) $p = 2$ or $p \equiv \pm 1 (\mod 8)$.

4. Prove that a positive integer n can be written as $n = |a^2 - 2b^2|$ for $a, b \in \mathbb{Z}$ iff any prime of the form $8k \pm 3$ occurs in the prime factorisation of n an even number (0 also allowed) of times.

5. How many solutions does $x^2 - 2y^2 = 850$ have for $x, y \in \mathbb{Z}$? How about $x^2 - 2y^2 = 851 = 23 \cdot 37$?

Solution:

1. Pick any $\alpha, \beta \in R, \beta \neq 0$. Then $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{2})$, and we can write it as $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = q_1 + q_2\sqrt{2}$. Then we can find $m, n \in \mathbb{Z}$ such that $|q_1 - m| \leq \frac{1}{2}, |q_2 - n| \leq \frac{1}{2}$. Therefore, see that

$$|\frac{\alpha}{\beta} - (m + n\sqrt{2})| = |q_1 - m + \sqrt{2}(q_2 - n)| \leq \left(\frac{1}{2}\right)^2 + \sqrt{2}\left(\frac{1}{2}\right)^2 < 1.$$

   Thus we have $\left|\frac{\alpha}{\beta} - (m + \sqrt{2}n)\right| < 1 \implies \left|\alpha - \beta(m + \sqrt{2}n)\right| < |\beta|$. Setting $\left|\alpha - \beta(m + \sqrt{2}n)\right| = r$, we have our answer.

2. Let π be a prime in R. Then $\pi\overline{\pi} = p_1 \dots p_k$, where $p_1, \dots, p_k$ are primes in R. Since π and $\overline{\pi}$ are conjugates, and they are primes themselves, k can be at most 2. In the case where $k = 1$, we have the case that $\pi\overline{\pi} = p$. Thus we have $|\pi\overline{\pi}| = p$. In the case where $k = 2$, we have $\pi\overline{\pi} = p_1 p_2$. Let $\pi | p_1$, then we must have $\overline{\pi} | \overline{p_1}$. If $p_1 = \overline{p_1}$, then $p_1 = p_2 = p \in \mathbb{Z}$. If $p_2 = \overline{p_1}$, we can also see that $p_1 = \overline{p_2}$ by the same argument using $\overline{\pi} | p_2$. Then we have $p_1 = p_2 = p \in \mathbb{Z}$. This means that π must be an associate of a prime in $\mathbb{Z}$.

3. (a) (a) $\implies$ (b): Let us assume that p splits in R, that is, $p = |\alpha\overline{\alpha}|$, where $\alpha = a + \sqrt{2}b \in R$. Now see that we have $p = |a^2 - 2b^2|$. This means that $a^2 - 2b^2 \equiv 0 \mod p$. Since $\mathbb{F}_p$ is a field, we know that b^{-1} exists for $b \neq 0$. $b = 0$, is simply not possible, as that would imply that $p = a^2$, which means that p is not prime. As b must be invertible, we see that $(b^{-1})^2(a^2 - 2b^2) = (ab^{-1})^2 - 2 \equiv 0 \mod p$. Then, see that ab^{-1} is a solution for $x^2 - 2 = 0$ in $\mathbb{F}[x]$.

   (b) (b) $\iff$ (c): Assume true.

   (c) (b) $\implies$ (a): We will prove the contrapositive. Let us say that p does not split in R. Then we have that p is prime in R. Then see that

$$\frac{\mathbb{Z}[\sqrt{2}]}{(p)} \cong \frac{\mathbb{Z}[x]}{(x^2 - 2, p)}$$

   is a domain. Then

$$\frac{\mathbb{Z}[x]}{(x^2 - 2, p)} \cong \frac{\mathbb{F}_p[x]}{(x^2 - 2)}$$

   is a domain. Since $\mathbb{F}_p[x]$ is a PID, $(x^2 - 2)$ which is a prime ideal must now also be irreducible. Therefore there is no root of $x^2 - 2$ in $\mathbb{F}_p[x]$

4. We know from the previous problem that the primes p in $\mathbb{Z}$ that split in R are of the form $8k \pm 1$ or the special case $p = 2$. We know that the other cases ($p = 8k \pm 3$) are inert; that is, they are prime in R. This is assumed from the previous question. We write the integer $n \in \mathbb{Z}$ as a product of primes, that is, $n = \prod_{i=1}^{k} p_i^{k_i}$, where $k_i > 0$. The power of the primes that split are of no concern since they can be written in the form $|a^2 - 2b^2|$ anyway. However, one needs to check that the product of any two terms of the form $|a^2 - 2b^2|$ also results in an expression of the same form. This is evident from the fact that if p and q are two prime numbers such that $p = |a^2 - 2b^2|, q = |c^2 - 2d^2|$, then $pq = |(a + \sqrt{2}b)(c + \sqrt{2}d) \cdot \overline{(a + \sqrt{2}b)(c + \sqrt{2}d)}| = |(ac + 2bd)^2 - 2(bc + ad)^2|$. Then the product of any two such primes of this form should also be of the same form. We can naturally say this about any finite product of such primes.

   Now assume that p_1 is a prime of the form $8k \pm 3$, and that it is the only such prime in n. Then we have $n = p_1^{k_1}|a^2 - 2b^2|$, where $|a^2 - 2b^2|$ is a product of the primes that split. Then n can be written in the required form only if $k_1 \equiv 0 \mod 2$, that is, it occurs even number of times. We can easily extend this to any n, by saying that for all primes of the form $8k \pm 3$, they should turn up even number of times in the prime factorisation of n.

   Conversely, we have for $n \in \mathbb{Z}$, primes of the form $8k \pm 3$ turn up even number of times. Let all other primes that split be split, and the resulting expression shall be written as $|a^2 - 2b^2|$. Then let $p_1, \ldots, p_s$ denote all those primes that remain inert. We know that $k_1, \ldots, k_s$, their respective powers are all even, thus $\prod_{i=1}^{s} p_i^{k_i} = \ell^2$, where $\ell := \prod_{i=1}^{s} p_i^{\frac{k_i}{2}}$. Then see that $n = |(an)^2 - 2(bn)^2|$, which proves our claim.

5. In the first, $n = 850 = 2 \cdot 5^2 \cdot 17$. 2 and 17 are both primes that split as they are 2 and $8 \cdot 2 + 1$ respectively, and 5 is inert since it is $8 \cdot 1 - 3$. It turns up twice, so we know that 850 can be written as $|a^2 - 2b^2|$ in at least one way. The powers of the two splitting primes are both 1, hence we can either choose to split them or not split them. However, not splitting is not an option since without splitting, the remaining portion has to have even power, which is not possible. Thus 2 and 17 must both be split. Note that $1 + \sqrt{2}$ is a unit; a fortiori, any integer power of $1 + \sqrt{2}$ is also a unit. Thus it is possible to write $1 = (1 + \sqrt{2})^n(1 + \sqrt{2})^{-n} = (1 + \sqrt{2})^n(-1 + \sqrt{2})^n$ in infinitely many ways(Note that $(1 + \sqrt{2})^{-1} = (-1 + \sqrt{2})$). Thus we can write 850 as $1 \cdot \pi_1 \cdot \overline{\pi_1} \cdot \pi_2 \cdot \overline{\pi_2} \cdot 5^2$, where $2 = \pi_1\overline{\pi_1}$ and $17 = \pi_2\overline{\pi_2}$. Then see that $850 = (1 + \sqrt{2})^{2n} \cdot 5^2 \cdot (-1 + \sqrt{2})^{2n}(a^2 - 2b^2) = (5(1 + \sqrt{2})^n)^2(\alpha^2 - 2\beta^2) = (5(1 + \sqrt{2})^2\alpha)^2 - 2(5(1 + \sqrt{2})^2\beta)^2$, which means that we have infinitely many ways to express 850 in the required form.

   When $n = 851 = 23 \cdot 37$, we have $37 = 8 \cdot 5 - 3$, which appears an odd number of times. Thus 851 cannot be written in the form $|a^2 - 2b^2|$.

3

1. Let R be a UFD. Suppose $I \subseteq R[x]$ is an ideal containing two nonzero elements f, g having no common factor. Prove that I contains a nonzero constant, i.e., and element of $R \backslash \{0\}\}$.

2. Let R be a PID and $f, g \in R[x]$ be 2 nonzero polynomials having no common factor. Prove that there are only finitely many prime ideals in $R[x]$ containing f and g. Moreover, any such prime ideal is maximal and is of the type $(p, h(x))$, where p is a nonzero prime element of R and $\overline{h(x)} \in \frac{R}{pR}[x]$ is irreducible.

3. Let R be a PID. Prove that any prime ideal $\mathfrak{p}$ in $R[x]$ is in one of the two following forms:

   (a) $\mathfrak{p} = (0)$,

   (b) $\mathfrak{p} = (f(x))$, for some irreducible polynomial f,

   (c) $\mathfrak{p} = (p, h(x))$, where $p \in R\backslash\{0\}$ is a nonzero prime element of R and R and $\overline{h(x)}$ is irreducible modulo p.

   Moreover the primes in (iii) are maximal.

4. Let F be an algebraically closed field and f a non-constant polynomial in $F[x, y]$. Prove that f has at least one zero in in F^2. Deduce that every maximal ideal $\mathfrak{m}$ in $F[x, y]$ is of the form $(x - a, y - b)$ for some $a, b \in F$.

5. Let F be as in the previous question and let $f, g \in F[x, y]$ be nonzero polynomials with no common factors. Prove that $\mathcal{Z}(f) \cap \mathcal{Z}(g)$ is a finite set where $\mathcal{Z}(-)$ denotes the zeroes in F^2 of a polynomial in $F[x, y]$.

6. Let $R = F[[t]]$ where F is a field or let $R = \mathbb{Z}\left[\left\{\frac{1}{p}\right\}\right]$ where p ranges over all the odd prime numbers. Prove that there is a maximal ideal $\mathfrak{p} \subseteq R[x]$ that is principal.

Solution:

1. We are told that f and g have no common factor. If we find their gcd in $Q[x]$, where Q is the field of fractions of R, we see that $f(x)q_1(x) + g(x)q_2(x) = d(x)$, where $d(x)$ is the greatest common divisor of f and g in $Q[x]$. As we are told, they do not have a common factor, which implies that the gcd of d is 1. Now, since $q_1, q_2 \in Q[x]$, there exists a $c \in R\backslash\{0\}$ such that $cq_1, cq_2 \in R[x]$. This is just multiplying out the denominators in a rational polynomial. Thus see that $f(x)(cq_1)(x) + g(x)(cq_2)(x) = c$. Since $f, g \in I$, where I is an ideal in $R[x]$, $f \cdot a + g \cdot b \in I$, where $a, b \in R[x]$. Thus we have $f(x)(cq_1)(x) + g(x)(cq_2)(x) = c \in I$.

2. We need to first see that if $\mathfrak{p}$ is a prime ideal in $R[x]$, $\mathfrak{p} \cap R$ is a prime ideal in R. If for $a, b \in R[x]$ we have $ab \in \mathfrak{p} \cap R$, then we have $ab \in \mathfrak{p}$ and $ab \in R$. Since a, b are polynomials, their product being a scalar is only possible if $a, b \in R$. From primality of $\mathfrak{p}$, we have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Putting this together with the previous inference, $\mathfrak{p} \cap R$ is a prime ideal.

   We know that R is a PID, thus $\mathfrak{p} \cap R$, a prime ideal is generated by p, a prime element in R. We know that this intersection is non-empty from the previous section, since we know that a nonzero scalar lies in an ideal generated by f and g, two coprime polynomials. We know that $\frac{R[x]}{\mathfrak{p}}$ is a domain. Reducing this by (p), we have

$$\frac{R[x]}{\mathfrak{p}} \cong \frac{R[x]/(p)}{\mathfrak{p}/(p)} \cong \frac{\overline{R}[x]}{\overline{\mathfrak{p}}}$$

   is also a domain. Since $\overline{R}[x]$ is a PID, as it is the polynomial ring of a field, then we have $\overline{\mathfrak{p}}$ is also irreducible, since prime ideals are also irreducible in a PID. This means that such a prime ideal is of the form $(p, h(x))$ where $h(x)$ is irreducible in $\overline{R}[x]$, and p is a prime in R. We know that any prime ideal I containing f and g is such that $I \cap R = (p)$, where p is a prime. We say that $(f, g) \cap R = (\alpha)$, for some $\alpha \in R$. See that $p \mid \alpha$, for which have only finitely many choices. Now consider $\overline{I}$, which is I reduced by p. We know that $I = (p, h(x))$, thus we must have $\overline{h(x)}|\overline{f(x)}$ or $\overline{h(x)}|\overline{g(x)}$. This must also leave us with finitely many choices for $h(x)$, which implies that only finitely prime ideals exist that contain f and g.

3. Let $\mathfrak{p}$ be a prime ideal. Assume that $\mathfrak{p} \neq (0)$. Then if $\mathfrak{p}$ is a principal ideal, then it must be of the form $(f(x))$, where f is prime in $R[x]$. If not, we see that for $f \in \mathfrak{p}$, we consider the prime decomposition of f. Then at least one of them must lie in $\mathfrak{p}$. Let that element be f'. Then $(f') \subsetneq \mathfrak{p}$, thus there exists $g \in \mathfrak{p}$ such that $g \notin (f')$. Then we must have that f' and g have no common factors. Thus from the previous section we must have that this prime ideal is of the form $(p, h(x))$.

4. Take $f(x, y) \in F[x, y]$, a non-constant polynomial. Then fix either x or y, which yields a non-constant polynomial. Let us fix $x = a \in F\backslash\{0\}$, then $f(a, y) \in F[y]$ must have at least one root, say $y = b$, as this is a polynomial over an algebraically closed field. Thus $f(x, y)$ has (a, b) as a root. We now wish to characterise the maximal ideals in $F[x, y]$. For a fixed $a, b \in F$, $(x - a, y - b)$ is maximal. See that the surjective map $\phi : F[x, y] \to F$ such that $f(x, y) \mapsto f(a, b)$ must have a kernel containing $(x - a, y - b)$, as $x - a$ and $y - b$ are zero at (a, b). To see that this is in fact the kernel of this map, we consider any $f(x, y) \in \ker \phi$. Then we apply the division algorithm on $f(x, y)$ and $(x - a)$. We have $f(x, y) = q_(x, y)(x - a) + r_1(y)$. Since degree of x in r_1 must be less than 1, we have that r_1 is solely a polynomial in y. We know that evaluated at (a, b) we get $0 = 0 + r_1(b)$. Since

$r_1(b) = 0$, we must have $y - b \mid r_1(y)$. This means that $r_1(y) = (y-b)q_2(y)$. Putting all of this together, we have $f(x,y) = (x-a)q_1(x,y) + (y-b)q_2(y) \in (x-a, y-b)$. Thus we know that $\ker \phi = (x-a, y-b)$. Thus we have

$$\frac{F[x,y]}{(x-a,y-b)} \cong F.$$

As F is a field, $(x-a, y-b)$ is maximal.

Let $\mathfrak{m}$ be a maximal ideal. Then $\frac{F[x,y]}{\mathfrak{m}} \cong F$, from the weak Hilbert Nullstellensatz. Then we have $x + \mathfrak{m} = a \in F$, and $y + \mathfrak{m} = b \in F$. Thus see that $x - a \in \mathfrak{m}, y - b \in \mathfrak{m}$. This means that $(x-a, y-b) \subseteq \mathfrak{m}$, which is a maximal ideal contained in a maximal ideal. This only makes sense if $\mathfrak{m} = (x-a, y-b)$.

5. We know that for $(a,b) \in \mathcal{Z}(f) \cap \mathcal{Z}(g)$, we have $f(x,y) \in (x-a, y-b)$, and $g(x,y) \in (x-a, y-b)$. $(x-a, y-b)$ is a maximal ideal (and hence prime ideal) containing f and g, hence there must be only finitely many prime ideals that contain this one. Each such prime ideal corresponds to a common root of f and g, which means that they can only have finite number of roots in common.

6. When $R = F[[t]]$, then the ideal $(tx-1)$ is principal, and we know that $R[x]/(tx-1) \cong R[1/t] \cong Q(R)$, which is a field, implying that $(tx-1)$ is maximal. Similarly for $R = \mathbb{Z}\left[\left\{\frac{1}{p}\right\}\right]$, we take the ideal $(2x-1)$ which is principal. Moreover, $R[x]/(2x-1) \cong R[1/2] \cong \mathbb{Q}$, which is a field. This means that $(2x-1)$ is maximal.