MATH 123: HW 4 SOLUTIONS AND COMMENTS

DORA WOODRUFF

1. Problem 1

1.1. **Comments:** None in particular; people did well on this question! The trick of noticing that $\sigma(a) = |aa'|$ cleans up some computations.

1.2. **Solution:** Notice that $\sigma(a) = |aa'|$, where $a' = x - y\sqrt{3}$. So, we have

$$\sigma(ab) = |ab(ab)'| = |aa'bb'| = \sigma(a)\sigma(b)$$

We can write

$$\frac{a}{b} = x_1 + x_2\sqrt{3}$$

where $x_1, x_2 \in \mathbb{R}$. We can always find, for any real x, $n \in \mathbb{Z}$ such that $|x - n| \leq \frac{1}{2}$. Choose such n_1, n_2 for x_1, x_2, and consider $c = n_1 + n_2\sqrt{3}$. Notice that
$\sigma(\frac{a}{b} - c) = \sigma(\frac{a}{b} - (n_1 + n_2\sqrt{3})) = \sigma((x_1 - n_1) + (x_2 - n_2)\sqrt{3}) = |(x_1 - n_1)^2 - 3(x_2 - n_2)^2| \leq \max((x_1 - n_1)^2, 3(x_2 - n_2)^2) \leq \frac{3}{4}$

So, we can write $a = bc + r$ where $\sigma(r) = \sigma(a - bc) = \sigma(b)\sigma(\frac{a}{b} - c) \leq \frac{3}{4}\sigma(b) < \sigma(b)$ as desired.

Date: Spring 2023.

2. Problem 2

2.1. **Comments:** There was some confusion related to what $I + J = A$ means (it does *not* mean that each element of A can be expressed *uniquely* as a sum of an element of I and an element of J, nor does it mean that I and J do not intersect - they must intersect at 0 at least!)

2.2. **Solution:** a) Choose $(m, n) \in A/I \times A/J$ (where $m, n \in A$ are chosen as representatives of cosets). Since $I + J = A$, we can write $m = i_1 + j_1$, $n = i_2 + j_2$ for $i_x \in I, j_x \in J$. Then, $\phi(j_1 + i_2) = (m, n)$, because $j_1 + i_2 = m \mod I$ and $j_1 + i_2 = n \mod J$.

b) Our polynomial should have $\sqrt{2}$ as a root, and should give 1 when we plug in i. $x^2 - 2$ has $\sqrt{2}$ as a root, and gives -3 when we plug in i, so dividing by -3, a good choice is $p(x) = -\frac{1}{3}(x^2 - 2)$.

3. Problem 3

3.1. **Comments:** I was a little nitpicky here; this kind of argument doesn't work in an arbitrary ring, so your proof should make it clear which specific properties of $K[x]$ you are using. E.g. if you assumed without justifying at all that $\prod p_i + 1$ is divisible by some irreducible, I may have taken off a point.

3.2. **Solution:** Suppose for contradiction that there are finitely many monic, irreducible polynomials $p_1(x), p_2(x) \dots p_n(x) \in K[x]$. There is definitely at least one, for example $p(x) = x$, so we can take $P(x) = 1 + \prod_i p_i(x)$. $P(x)$ is still monic. Since $K[x]$ is a UFD, we can factor $P(x)$ into prime elements, which must be irreducible polynomials in $K[x]$ (and we can assume they are monic, since K is a field and $P(x)$ is monic). However, since $p_i(x)$ does not divide 1, $p_i(x)$ cannot divide $P(x)$, so some monic irreducible not from our list must divide $P(x)$, which is a contradiction.

4. Problem 4

4.1. **Comments:** almost everybody got this problem right, but some solutions were more complicated than others; if you didn't notice that you could use Eisenstein's Criterion, you probably had to do something annoying. Also, several people seemed to think that the coefficients all have to be nonzero in order for Eisenstein's Criterion to apply, which is not true! The nice thing about 0 is that anything you want divides it...

4.2. **Solution:** Since $a > 1$ and $\mathbb{Z}$ is a UFD, some prime p divides a. Since a is squarefree, p^2 does not divide a, and p divides all non-leading coefficients since $p|0$. Therefore, applying Eisenstein's Criterion with p, we see that $x^n - a$ is irreducible. (Technically, as stated in the notes Eisenstein's Criterion is for polynomials in $\mathbb{Q}[x]$, but clearly if $x^n - a$ is irreducible over $\mathbb{Q}[x]$, it is irreducible over $\mathbb{Z}[x]$).

5. Problem 5

5.1. **Comments:** There were several ways to approach the first part, such as analyzing the coefficients of a product pq, but the cleanest way is to exploit the fact that $K[t]$ is a UFD. Similarly, you can approach the second part either by proving that $K[t, t^{-1}]$ is a Euclidean Domain, hence a PID, or by showing directly that it is a PID using the fact that $K[t]$ is a PID. The latter is quite a bit easier (coming up with a size function and an algorithm is a lot of work).
A very small mistake a lot of people made in this part was assuming that all ideals in $K[t, t^{-1}]$ are finitely generated, which is not clear a priori (such rings are called Noetherian, and not all rings are Noetherian). But all proofs that assumed this were easily alterable/didn't really rely on the assumption.

5.2. **Solution:** a) Elements of the form ct^k are definitely units, with inverse $c^{-1}t^{-k}$. We will show that these are the only units. Suppose $pq = 1$ in $K[t, t^{-1}]$. Choose $n, m \geq 0$ to be the smallest integers such that $t^n p, t^m q \in K[t]$. Then, we have that

$$(t^n p(x))(t^m q(x)) = t^{m+n} \in K[t]$$

Since $K[t]$ is a UFD, and t^{m+n} factorizes as the product of $m + n$ t's, we must have that $t^n p(x)$ and $t^m q(x)$ are both of the form ct^k, as desired.

b) Let $I \subset K[t, t^{-1}]$ be an ideal. Consider $I \cap K[t]$, which is an ideal of $K[t]$. $K[t]$ is a PID, so $I \cap K[t] = (p)$ for some p. However, for any $q \in I$, for large enough N we have $t^N q \in K[t]$, so $t^N q = hp$ for some $h \in K[t]$. Then, we have $q = t^{-N} hp$, so q is a multiple of p too. Therefore, p generates I in $K[t, t^{-1}]$, as desired.

6. Problem 6 (Bonus)

6.1. **Comments:** The most common errors were just not checking details: e.g. it does not suffice to check that $\phi(x^2+y^2-1)=0$ to conclude that $(x^2+y^2-1)=\ker(\phi)$ (you need to justify why $(x^2+y^2-1)\supset\ker(\phi)$ too).

6.2. **Solution:** a) We consider the surjective homomorphism $\phi:\mathbb{R}[x,y]\to A$ given by sending $x\to\cos(t)$ and $y\to\sin(t)$. By the First Isomorphism Theorem, we want to show that $\ker(\phi)=(x^2+y^2-1)$. Since $\cos^2(t)+\sin^2(t)=1$, we know $(x^2+y^2-1)\subset\ker(\phi)$, so it suffices to show that $\ker(\phi)\subset(x^2+y^2-1)$.

Suppose that $\phi(p(x,y))=0$. Using the relation $x^2+y^2-1=0$, we can rewrite $p(x,y)=q(y)+xh(y)$. Since $h(y)=0$ for only finitely many values of y, we must have that $x=-\frac{q(y)}{h(y)}$, and therefore that $y^2+\frac{q(y)^2}{h(y)^2}=1$, for infinitely many values of y. Thus,

$$q(y)^2+(y^2-1)p(y)^2=0$$

for infinitely many y. But then, we must have that the left side is the zero polynomial, and since (y^2-1) is not the square of a polynomial, $q(y)$ and $p(y)$ must both be $0 \mod x^2+y^2-1$, as desired.

b) It suffices to show that (y) is irreducible but not prime, as irreducibles are prime in a UFD. $\mathbb{R}[x,y]/(x^2+y^2-1,y)\simeq\mathbb{R}[x]/(x^2-1)$ is not an integral domain, since $x+1$ and $x-1$ are nontrivial zero divisors, so y is not prime. Now, we want to show that the only principle ideals containing (y) are (y) and (1). Suppose that (y) is contained in (p). As before, we can write each polynomial in the form $g(y)x+h(y)$ by replacing each instance of x^2 with $1-y^2$. Let $p(x,y)=a(y)x+b(y)$. Since $y\in(p)$, we must have

$$(a(y)x+b(y))(c(y)x+d(y))=a(y)c(y)(1-y^2)+(c(y)b(y)+a(y)d(y)x+b(y)d(y))=y$$

So, $c(y)b(y)+a(y)d(y)=0$ and since $\mathbb{R}[y]$ is a UFD, we can write $a(y)=-f(y)a'(y)$ (and similarly for $b(y),c(y),d(y)$). Furthermore, we have

$$a(y)c(y)(1-y^2)+b(y)d(y)=y$$

so

$$f(y)g(y)(a'(y)^2(y^2-1))+b'(y)^2)=y$$

If $a'(y)$ is nonzero, then the degree of $a'(y)^2(y^2-1)+b'(y)^2$ must be at least 2. So, $a'(y)=0$. Thus, we get $b(y)d(y)=y$, and so up to signs, $p(y)=y$ or $p(y)=1$. Thus, (y) is irreducible.

c) We can consider the homomorphism $\mathbb{C}[t,t^{-1}]\to\mathbb{C}[x,y]/(x^2+y^2-1)$ given by $t\to x+iy$ (and thus $t^{-1}\to x-iy=(x+iy)^{-1}$). In the other direction, we have the homomorphism $\mathbb{C}[x,y]/(x^2+y^2-1)\to\mathbb{C}[t,t^{-1}]$ given by $x\to\frac{t+t^{-1}}{2}, y\to\frac{t-t^{-1}}{2}$. It can be easily checked by hand that these two homomorphisms are inverses of each other, and hence $\mathbb{C}[x,y]/(x^2+y^2-1)\simeq\mathbb{C}[t,t^{-1}]$, which is a PID, hence UFD, by Problem 5.