Selected Math 553 Homework Solutions

HW6, 1. Let α and β be rational numbers, with $|\alpha| \le 1/2$, and let $m > 0$ be an integer such that $\alpha^2 - m\beta^2 = -1 - \delta$ where $0 \le \delta < 1$. Set $\epsilon := 1$ if $\alpha \ge 0$ and -1 if $\alpha < 0$. Show that if m is not of the form $5n^2$ $(n \in \mathbb{Z})$ then $|(\alpha + \epsilon)^2 - m\beta^2| < 1$.

Deduce that $\mathbb{Z}[\omega]$ is norm-Euclidean when $\omega = \sqrt{6}$, when $\omega = \sqrt{7}$, or when $\omega^2 - \omega + q = 0$ with $q = -4$,-5 or -7.

Solution.

It holds that

$$(\alpha + \epsilon)^2 - m\beta^2 = (\alpha^2 - m\beta^2 + 1) + 2\alpha\epsilon = -\delta + 2\alpha\epsilon = -\delta + 2|\alpha|,$$

and that

$$-1 < -\delta + 2|\alpha| \le -\delta + 1 \le 1,$$

so that $|(\alpha + \epsilon)^2 - m\beta^2| \le 1$, with equality only if $\delta = 0$ and $\alpha = \pm 1/2$—in which case $m\beta^2 = \alpha^2 + 1 = 5/4$, whence $m = 5n^2/q^2$ for some relatively prime integers n and $q \ne 0$; and since q^2 divides $5n^2$ therefore q^2 divides 5, forcing $q^2 = 1$, i.e., $m = 5n^2$, which is excluded by assumption.

Let's deduce that $\mathbb{Z}[\sqrt{m}\,]$ is norm-Euclidean when $m = 6$ or 7. (The argument will also cover the cases $m = 2$ and $m = 3$, treated previously in class.)

We need that any $u + v\sqrt{m}$ where u and v are rational has a "good approximation" $a + b\sqrt{m}$ $(a, b \in \mathbb{Z})$, that is, if $\alpha := a - u$ and $\beta := b - v$ then

$$|\alpha^2 - m\beta^2| < 1. \tag{1.1}$$

Choose $a, b \in \mathbb{Z}$ such that $|a - u| \le 1/2$ and $|b - v| \le 1/2$. If (1.1) holds, fine. (This always happens for $m = 2$ or 3.) If not, then since $m < 8$ therefore $\alpha^2 - m\beta^2 = -1 - \delta$ where $0 \le \delta < 1$, and the above result shows that (1.1) will hold after a is replaced by $a + \epsilon$.

As for $\mathbb{Z}[\omega]$ where $\omega^2 - \omega + q = 0$ $(q < 0)$, we need that, with preceding notation,

$$\begin{aligned} 1 > \operatorname{Norm}\big((a-u) + (b-v)\omega\big) &= (a-u)^2 + (a-u)(b-v) + q(b-v)^2 \\ &= \left((a-u) + \frac{b-v}{2}\right)^2 - (1-4q)\left(\frac{b-v}{2}\right)^2 > -1. \end{aligned} \tag{1.2}$$

Set $m := 1 - 4q$, $\beta := (b - v)/2$, $\alpha := a + b - u$, choosing $b \in \mathbb{Z}$ so that $|\beta| \le 1/4$, and then $a \in \mathbb{Z}$ so that $|\alpha| \le 1/2$. As above, (1.2) is satisfied—after replacement of a by $a + \epsilon$, if necessary—as long as $\alpha^2 - m\beta^2 > -2$ and $m \ne 5n^2$, which does hold if $q = -4$,-5 or -7 (and also in the cases $q = -2$ and $q = -3$, treated previously in class).

HW6, 2. (Fermat). Find all solutions in positive integers of the equation $y^3 = x^2 + 4$.

Hint. Prove and use the following facts about Gaussian integers.
(i) $a + bi$ is divisible by $1 + i \iff a - b$ is even.
(ii) If $y^3 = x^2 + 4$ $(x, y \in \mathbf{Z})$, then

$$(x + 2i,\, x - 2i) = \begin{cases} 1 & \text{if } x \text{ is odd} \\ (1 + i)^3 & \text{if } x \text{ is even.} \end{cases}$$

(iii) If $y^3 = x^2 + 4$ then $x + 2i = i^n(a + bi)^3$ for some n, a, b.

Solution. First, the hints.

(i) For given $a, b \in \mathbb{Z}$, there exist $c, d \in \mathbb{Z}$ such that

$$a + bi = (c + di)(1 + i) = (c - d) + (c + d)i$$

iff the equations $c - d = a$, $c + d = b$ can be solved in $\mathbb{Z}$, i.e., iff $(a + b)/2$ and $(a - b/2$ are in $\mathbb{Z}$, i.e., iff $a - b$ is even.

(ii) Any common factor p of $(x + 2i)$ and $(x - 2i)$ divides their difference, which is $4i = -i(1+i)^4$, so p must be an associate of $(1+i)^n$ $(0 \le n \le 4)$. (Note that $1+i$ has prime norm 2, so that $1+i$ is prime.) If x is odd then by (i), $(x+2i)$ is not divisible by $(1+i)$, so p is a unit. If x is even, say $x = 2z$, then z must be odd (otherwise both y^3 and x^2 would be divisible by 8, contradicting $y^3 - x^2 = 4$), and so

$$(x + 2i,\, x - 2i) = 2(z + i, 1 + i) = (1 + i)^3.$$

(iii) Since $(x + 2i)(x - 2i) = y^3$, and every unit in $\mathbb{Z}[i]$ is a cube, we see that if $x + 2i$ and $x - 2i$ are relatively prime, i.e., x is odd, then for some $a, b \in \mathbb{Z}$, $(x + 2i) = (a + bi)^3$. When x, and hence y is even, say $y = 2w$, then

$$\frac{x + 2i}{(1 + i)^3}\,\frac{x - 2i}{(1 + i)^3} = \frac{y^3}{-8i}\,,$$

and since the two factors on the left are relatively prime, it follows easily that, again, $(x + 2i) = (a + bi)^3$ for some a and b.

Thus

$$x + 2i = (a + bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i,$$

so that $x = a(a^2 - 3b^2)$ and $b(3a^2 - b^2) = 2$. The latter equality forces $b = 1$ and $a = \pm 1$ or $b = -2$ and $a = \pm 1$, giving, respectively, $\boxed{x = 2,\ y = 2,}$ or $\boxed{x = 11,\ y = 5.}$

HW8, 1. Let R be a UFD, with fraction field K. Suppose you already have computer algorithms for factoring into primes in R and in the polynomial ring $K[X]$. Describe briefly how you would instruct a computer to factor into primes in $R[X]$.

Solution. Given a polynomial $p \in R[X]$, factor it into primes in $K[X]$. Represent each prime $K[X]$-factor in the form $(c_i/d_i)p_i$ with $c_i, d_i \in R$, and $p_i \in R[X]$ *primitive*, i.e., the gcd of the coefficients of p_i is 1. (Any polynomial $q \in K[X]$ has the form $(1/d)q'$ with $q' \in R[X]$; and $(1/d)q' = (c/d)q^*$ where $c =$ gcd of the coefficients of q'—determined by factoring them into primes, whence $q^* \in R[X]$ is primitive.) So

$$p = \prod_{i=1}^{n} \frac{c_i}{d_i} p_i = \frac{c}{d} \prod_{i=1}^{n} p_i \qquad \Bigl(\text{where } c = \prod_{i=1}^{n} c_i,\ d = \prod_{i=1}^{n} d_i\Bigr). \tag{2.1}$$

What is usually called *Gauss's Lemma*, shown by arguing as in the proof of Proposition 5 on p. 303 of D&F, is the assertion that *any product of primitive polynomials is primitive.* It follows that in (2.1), c is the gcd of the coefficients of dp, whence $d|c$ in R.

Since $R[X]$ is a UFD, Corollary 6 on p. 304 of D&F gives that each p_i is prime in $R[X]$. And by Proposition 2 on p. 296 of D&F, every prime element in R is prime in $R[X]$. Thus a prime factorization of p can be gotten from (2.1) by factoring c/d into primes in R.

HW8, 2. Let k be a field, x, y, and z indeterminates.

(a) Let $f(x)$ and $g(x)$ be relatively prime polynomials in $k[x]$. Show that in the polynomial ring $k(y)[x]$, $f(x) - yg(x)$ is irreducible.

(b) Prove that in $k(y,z)[x]$, the polynomial

$$x^4 - yzx^3 + (y^2z^2 - y)x^2 + (y^2z - y)x + y^2z$$

is irreducible. (Hint. Eisenstein, after rearranging.)

Solutions. (a) By Proposition 5 on p. 303 of D&F, it suffices that $f(x) - yg(x)$ be irreducible in $k[y][x] \cong k[y,x] \cong k[x,y] \cong k[x][y]$, which it is, by Corollary 6 on p. 304 of D&F, because it is primitive in $k[x][y]$ and irreducible in $k(x)[y]$ (its degree being 1).

(b) The polynomial can be viewed as the primitive polynomial

$$x^2y^2z^2 - y(x^3 - yx - y)z + x(x^3 - yx - y) \in k[x,y][z],$$

to which one applies Eisenstein's criterion with the prime $x^3 - y(x+1) \in k[x,y]$ (see (a)) to get irreducibility in $k[x,y][z] \cong k[y,z][x]$, whence in $k(y,z)[x]$ (by Proposition 5 on p. 303 of D&F). Note that Proposition 13 on p. 309 isn't quite good enough, because it refers to a monic polynomial; but pretty much the same argument applies to any primitive polynomial $a_nx^n + a_{n-1}x^{n-1} + \dots$ with $a_n \notin P$ (the prime ideal in Prop. 13).

HW8, 3. Let R be an integral domain with fraction field K, let $R[X]$ be a polynomial ring, and let a and b be nonzero elements in R. Prove:

(a) If R is a UFD and $P \subset R[X]$ is a prime ideal with $P \cap R = (0)$, then P is a principal ideal.

(b) $aR \cap bR = abR$ iff the ring $R[X]/(aX - b)$ is an integral domain.

(c) If $c = aq = bp$ is a nonzero common multiple of a and b then c is an l.c.m. of a and b iff $pX - q$ is a prime element in $R[X]$.

(d) An l.c.m. $[a, b]$ exists iff the kernel of the R-homomorphism $\phi\colon R[X] \to R[\frac{b}{a}] \subset K$ taking X to $\frac{b}{a}$ is a principal ideal.

Solutions. (a) The $K[X]$-ideal $PK[X]$ generated by P is principal, with generator, say, $q = (c/d)q^*$ (see solution to 2 above), and then the primitive polynomial $f := q^*$ is also a generator. Being in $PK[X]$, f has the form $\sum h_i f_i$ with $h_i \in K[X]$ and $f_i \in P$, from which follows that $af \in P$ for some $a \neq 0 \in R$. As P is prime and $a \notin P$, therefore $f \in P$.

Now any $g \in P$ is a multiple of f in $K[X]$. But a careful reading of the proof of Proposition 5 on p. 303 of D&F shows that *if $p \in R[X]$ factors as $p = AB$ in $K[X]$, with B a primitive polynomial in $R[X]$, then $A \in R[X]$.* Thus g is a multiple of f in $R[X]$; and so P is generated by f.

(b) Suppose $aR \cap bR = abR$. Let $f(X)$ lie in the kernel of ϕ. In $R[\frac{1}{a}][X]$, a is a unit, so $f(X) = (aX - b)g(X) + c$; clear denominators to get that for some $n \geq 0$, $h \in R[X]$, and $r \in R$,

$$a^n f(X) = (aX - b)h(X) + r.$$

Set $X = b/a$ to see that $r = 0$. Now choose the least such n. Then if $n > 0$, the coefficients of $bg = aX - a^n f$ lie in $aR \cap bR = abR$, whence the coefficients of g are divisible by a. Hence $a^{n-1}f(X) = (aX - b)(a^{-1}h(X))$, contradicting the minimality of n. So $n = 0$ and $aX - b$ divides f. Thus the kernel of ϕ is generated by $aX - b$, and $R[X]/(aX - b)$ is isomorphic to the image of ϕ, clearly an integral domain.

Conversely, if the element $aX - b$ is prime in $R[X]$, and $d \in aR \cap bR = abR$, say $d = ap = bq$, then $p(aX - b) = b(qX - p)$ and $aX - b$ doesn't divide b, and so $aX - b$ divides $qX - p$, whence $a|q$ and $ab|qb = d$. Thus $aR \cap bR = abR$.

(c) Suppose $c = [a, b]$. Note that neither p nor q is 0, since $c \neq 0$. If x is a common multiple of p and q then bx is a common multiple of $bp = aq$ and of bq, so bx is a multiple of $cq = bpq$, whence x is a multiple of pq. Thus $[p, q] = pq$, or equivalently, $pR \cap qR = pqR$; and by (b), $pX - q$ is prime.

Conversely, if $pX - q$ is prime, so that by (b), $pR \cap qR = pqR$, i.e., $[p, q] = pq$, then $[pa, pb] = [qb, pb] = pqb$, whence $[a, b] = qb = c$.

(d) As in the proof of (c), if $c = aq = bp = [a, b]$, then $pR \cap qR = pqR$; so by (b), the kernel of $\phi\colon R[X] \to R[\frac{q}{p}] = R[\frac{b}{a}]$ is generated by $pX - q$.

Conversely, if the kernel of ϕ is principal, then since it contains $aX - b$ and no nonzero element of R, its generator, a prime element, must be of the form $pX - q$; and by (b), $pR \cap qR = pqR$, i.e., $[p, q] = pq$. Moreover, $aX - b = r(pX - q)$ for some $r \in R$. Hence

$$[a, b] = [rp, rq] = pqr.$$

HW8, 4. (a) Prove that if $x \neq 0$ and y are elements in a UFD such that x^2 divides y^2, then x divides y.

(b) Let k be a field. In the quotient ring $R = k[X,Y,Z]/(Y^2 - X^2 Z)$ let $x = \overline{X}$ and $y = \overline{Y}$ be the natural images of X and Y. Show that x^2 divides y^2 in R, but x does not divide y.

(c) Is R an integral domain? (Why?)

Solutions. (a) $\big[(x,y)^2 = (x^2, y^2) = x^2\big] \implies \big[(x,y) = x\big]$.

(b) Let $z = \overline{Z}$. Then $y^2 = x^2 z$. If $x|y$ then there are polynomials f and g such that

$$Y = Xf(X,Y,Z) + (Y^2 - X^2 Z)g(X,Y,Z).$$

Setting $X = 0$ produces a contradiction.

(c) Yes, because $Y^2 - X^2 Z$ is irreducible (primitive in $k[X,Y][Z]$ and irreducible in $k(X,Y)[Z]$), therefore prime (since $k[X,Y,Z]$ is a UFD).