David Akeley 110BH final

1A. $\mathbb{Z}[\sqrt{-1}]$ Euclidean Domain

Let $a, b \in \mathbb{Z}[\sqrt{-1}]$ be given, with $b \neq 0$

Define $q^\nabla = a/b$ in $\mathbb{C}$

Let $\delta: \mathbb{Z}[\sqrt{-1}] \to \mathbb{N}$ $\quad \delta(x+y\sqrt{-1}) \mapsto x^2+y^2$
define the Euclidean function. (i.e. let the $\mathbb{C}$-norm restricted to $\mathbb{Z}[\sqrt{-1}]$ be δ).

Pick $q \in \mathbb{Z}[\sqrt{-1}]$ so that q is near q^∇, i.e., with

$$q = x + y\sqrt{-1} \qquad q^\nabla = x^\nabla + y^\nabla\sqrt{-1}$$

we should have

$$|x - x^\nabla| \leq 1/2 \qquad |y - y^\nabla| \leq 1/2$$

Then set $r = b(q^\nabla - q)$, so that $r \in \mathbb{Z}[\sqrt{-1}]$ and

$$a = bq + r = bq + bq^\nabla - q = b\frac{a}{b} = a$$

Then

$$\delta(r) = |r| = |b||q^\nabla - q| = |b|\left((x-x^\nabla)^2 + (y-y^\nabla)^2\right)$$

Both $|x - x^\nabla| \leq \frac{1}{2}$ and $|y - y^\nabla| \leq \frac{1}{2}$, so

$$\delta(r) \leq |b|\frac{1}{2} < |b| = \delta(b)$$

Statement for test:

I did all this work by myself without aid from any sources

- David Alcivar

1B. $\mathbb{Z}[\sqrt{-1}, t]$ is not Euclidean.

Counterexample: $(2\sqrt{-1}, t)$ is not a principal ideal.
Hence $\mathbb{Z}[\sqrt{-1}, t]$ is not a PID, and not Euclidean.

---

2. Let $R = \mathbb{Z}[\sqrt{-d}]$, with $d \geq 3$ a square-free integer.

I claim 2 is irreducible but not prime in R.

Irreducible: Consider

$$(a+b\sqrt{-d})(x+y\sqrt{-d}) = 2 = ax + dby + (ay+bx)\sqrt{-d}$$

in R. We have $ay + bx = 0$, so $x = -ay/b$. Substitute into $ax + dby = 2$.

$$-a^2y/b + dby = 2$$

Irreducible: Consider if $xy = 2$ with $x, y \in \mathbb{Z}[\sqrt{-d}]$.
The $\mathbb{C}$ norm is multiplicative, so $|x||y| = 4$. Then, as the norm on $\mathbb{Z}[\sqrt{-d}]$ yields integers, either

$|x| = 4 \quad |y| = 1$
$|x| = 2 \quad |y| = 2$
$|x| = 1 \quad |y| = 4$

The $|x| = 2$ case is impossible though: all norms on $\mathbb{Z}[\sqrt{-d}]$ are of the form $a^2 + b^2 d$, with $a, b \in \mathbb{Z}$. This cannot be solved for 2 with $d \geq 3$. So either $|x| = 1$ or $|y| = 1$, and x or y is a unit. So 2 is irreducible.

2 continued

Prime: I claim 2 is not prime in R.

If d is odd, consider the product

$$(1+\sqrt{-d})(1-\sqrt{-d}) = 1+d$$

$1+d$ is divisible by 2 as d is odd, but neither operand is divisible by 2 (note $2(x+y\sqrt{-d}) = 2x+2y\sqrt{-d}$, so both the real and $\sqrt{-d}$ part must be even to be divisible by 2).

If d is even, then consider

~~$(2+\sqrt{-d})(2-\sqrt{-d})$~~ $\sqrt{-d}\cdot-\sqrt{-d} = d$

A similar argument applies.

Note: with $d \geq 3$, none of the above operands are units. They all have $\mathbb{C}$ norm ≥ 2.

Since 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-d}]$ with $d \geq 3$, $\mathbb{Z}[\sqrt{-d}]$ is not a UFD — we expect all irreducibles to be prime in UFDs.

I.4 (I'm not so sure about this one).

Let R be a UFD with quotient field F, and let f, g be primitive polynomials in $R[t]$. I claim

f, g are not relatively prime in $R[t]$ $\iff$ "f, g" " $F[t]$

($\Rightarrow$) If f, g are not relatively prime in $R[t]$, then
non-unit $\rightarrow$ $\exists h \in R[t]$ with $h \mid f$, $h \mid g$. h must have degree at least 1; ~~otherwise, f and g would not~~ f and g are primitive so no non-unit in R divides them. This $h \in R[t]$ is also a non-unit in $F[t]$ as $\deg h \geq 1$ and F is a domain. So $h \mid f$, $h \mid g$ in $F[t]$, and f, g are not relatively prime in $F[t]$.

($\Leftarrow$) I am not sure, but I think $R[t]$ is a UFD.

Pick some $f \in R[t]$, and factor f as a product of irreds.

$$f = r_1 \cdots r_m g_1 \cdots g_n$$

with $r_i \in R$, $g_i \in R[t] \setminus R$.

All the g_i must be primitive to be irreducible. So - this is the dubious part - $C(g_1 \cdots g_n) = 1$, and so $C(f) = r_1 \cdots r_m$.

r_1 through r_m are unique, as R is a UFD.
up to units

$g_1 \cdots g_n \in R[t] \setminus R \subseteq F[t]$ are unique up to units as $F[t]$ is a UFD (F: field).

I.4 continued.

Anyway, suppose f and g have a common divisor $h^0 \in F[t]$, with h^0 of deg ≥ 1. Write

$$h^0 = \frac{h}{k}$$

with $k \in R$ and $h \in R[t]$ primitive. We then have

$$\frac{h}{k} \mid f \Rightarrow h \mid kf \text{ in } R[t].$$

$$\frac{h}{k} \mid g \Rightarrow h \mid kg \text{ in } R[t].$$

There exist $a, b \in R[t]$ so that

$$ah = kf \qquad bh = kg$$

Factor k as irreducibles $k = p_1 \cdots p_n$. (Maybe should have been $p_1^{e_1} \cdots p_n^{e_n}$) Since $R[t]$ might be a UFD, p_i's are prime. From above, we see that

$$k \mid ah \text{ and } k \mid bh.$$

So every p_i divides ah and bh. h is primitive, so $p_i \mid a$ ($p_i^{e_i} \mid a$) $p_i \mid b$ ($p_i^{e_i} \mid b$) for all $p_i^{e_i}$. $k \mid a$ and $k \mid b$ then. Cancel k.

$$\frac{a}{k} h = f \qquad \frac{b}{k} h = g$$

So $h \mid f$, $h \mid g$ in $R[t]$, and as $\deg h \geq 1$, this shows f and g to not be coprime in $R[t]$.

I.6. Let R be a domain. With $\mathfrak{m}$ being a maximal ideal of R, let $R_{\mathfrak{m}} \subseteq \mathrm{Frac}(R)$ be the localization $R_{R\setminus\mathfrak{m}}$.

I claim that $R = \bigcap_{\mathfrak{m}\text{ maximal ideal in } R} R_{\mathfrak{m}}$

($\subseteq$) For every $r \in R$ and maximal ideal $\mathfrak{m} < R$, $r = \frac{r}{1} \in R_{\mathfrak{m}}$, as $1 \in R\setminus\mathfrak{m}$ for all $\mathfrak{m} < R$. So $R \subseteq \bigcap R_{\mathfrak{m}}$

($\supseteq$) Suppose $\frac{r}{s} \in \bigcap R_{\mathfrak{m}}$ (assume $\frac{r}{s}$ in reduced form, i.e. $\nexists x$ a non-unit $\mid r, \mid s$) with $s \neq r$, i.e. there exists some elt. of ~~elt $\frac{r}{s}$ of $\mathrm{Frac}(R)$~~ $\bigcap R_{\mathfrak{m}}$ that is in $\mathrm{Frac}(R)$ but not in R. As $s \neq r$, s is not a unit, and $(s) < R$. Let

$$\mathcal{Q} = \{ I : \text{ideal of } R \mid (s) \subseteq I < R \}$$

i.e. $\mathcal{Q}$ is the set of all proper ideals of R containing (s). $(s) \in \mathcal{Q}$ so $\mathcal{Q}$ is non-empty. $\mathcal{Q}$ is ordered by $\subseteq$.

Given a chain $Q_1 \subseteq Q_2 \subseteq Q_3 \subseteq \dots$ in $\mathcal{Q}$, the union $\bigcup Q_i$ is still in $\mathcal{Q}$. $1_R \notin Q_i \ \forall Q_i$, so $1_R \notin \bigcup Q_i$, and $\bigcup Q_i < R$. $(s) \subseteq Q_1$, so $(s) \subseteq \bigcup Q_i$. Finally, $\bigcup Q_i$ is an ideal:

Pick ~~$a, b \in Q_i$~~ $a, b \in \bigcup Q_i$. Then $a \in Q_x$, $b \in Q_y$ for some Q_x, Q_y. $Q_{\min(x,y)} \subseteq Q_{\max(x,y)}$, so

$$a + b \in Q_{\max(x,y)} \subseteq \bigcup Q_i,$$

$$ra \in Q_x \subseteq \bigcup Q_i$$

Anyway, every chain in $\mathcal{Q}$ has a maximal elt. $\bigcup Q_i$ in $\mathcal{Q}$.

I.6. By Zorn's Lemma, $\mathcal{Q}$ contains a maximal element. Call it I, this is a maximal ideal of R containing (s). Then $\frac{r}{s} \notin M_I$, as $s \notin R \setminus I$. So it cannot actually be the case that $\frac{r}{s} \in \mathrm{Frac}(R) \setminus R$ can be in $\bigcap R_m$, so $R \supseteq \bigcap R_m$. ($\frac{r}{s}$ in reduced form.)

Together with $R \subseteq \bigcap R_m$, this shows $R = \bigcap R_m$

I.7B Looking for some low-hanging fruit for the last few minutes

Let $\pi: R \to R/u$ be canonical epi. I claim

$$nil(\bar{R}) = \sqrt{u}/u.$$

Pick $x+u \in \sqrt{u}/u$. Then $x \in \sqrt{u}$ (or some such representative x can be chosen). So $x^n \in u$ for some $n \geq 1$. Then $(x+u)^n = x^n + u = 0+u$, and

$x+u \in nil(\bar{R})$. So $\sqrt{u}/u \subseteq nil(\bar{R})$.

The other direction is pretty much the same.

Pick $x+u \in nil(\bar{R})$. Then $(x+u)^n = 0+u$ for some $n \geq 1$.

So $x^n + u = 0+u$. Then $x \in \sqrt{u}$, $x+u \in \sqrt{u}/u$.

$nil(\bar{R}) \subseteq \sqrt{u}/u$.

Together, this shows $nil(\bar{R}) = \sqrt{u}/u$.

I.8. Let R be a commutative ring.

A. I claim that these 2 are equivalent:

1. R satisfies descending chain condition on ideals
2. R satisfies the minimum principle.

$1 \Rightarrow 2$ I'll prove the contrapositive. Let $S \neq \emptyset$ be a collection of ideals of R that do not satisfy the minimum principle. Pick some $\mathcal{U}_1 \in S$. Then $\mathcal{U}_1$ is not a minimal elt, so the claim

$$\text{If } \mathcal{U}_1 \supseteq B \text{ with } B \in S \text{ then } B = \mathcal{U}_1$$

must be false. (Some $B \in S$ with $\mathcal{U}_1 \supseteq B$ must exist, or the statement is vacuously true).

So pick $B < \mathcal{U}_1$ in S, and set $\mathcal{U}_2 = B$. Iterate to produce a descending chain

$$\mathcal{U}_1 > \mathcal{U}_2 > \cdots$$

So if 2 is not satisfied, 1 is not satisfied.

$2 \Rightarrow 1$ If R satisfies the minimum principle, then any descending chain of ideals

$$\mathcal{U}_1 \supseteq \mathcal{U}_2 \supseteq \mathcal{U}_3 \cdots$$

is a collection of ideals, and contains a minimal element $\mathcal{U}_n$. Then $\mathcal{U}_n \supseteq \mathcal{U}_{n+i}$ $\forall i \geq 1$, and so

$\mathcal{U}_n = \mathcal{U}_{n+i}$ $\forall i \geq 1$. R satisfies DCC.

I.8.B

If R is an artinian domain, then R must be a field.

Suppose for the sake of contradiction that R is an artinian domain but not a field. Then there exists a non-unit $0 \neq x \in R$. I claim that

(*) $$(x) > (x^2) > (x^3) > \cdots$$

Because R is a domain, x is not nilpotent. So (*) consists of nonzero ideals. Furthermore, each inclusion

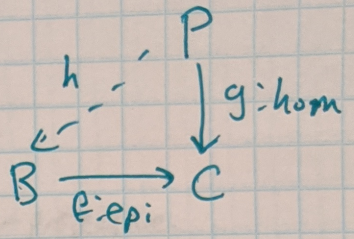
$$(x^{n+1}) \subseteq (x^n)$$

is strict; $x^n \notin (x^{n+1})$; otherwise there exists $b \in R$ so that $x^n = b x^{n+1}$, and, as we can cancel in domains, $1 = bx$ and $b = x^{-1}$ — contradicts x is non-unit.

Then (*) is a descending chain of ideals of R with no minimal element. This contradicts that R is an artinian domain.

II.1. Let P be an R-module

Let B, f, C, g be given →



A. If P is R-free, then P is R-projective.

Let $\{e_i\}$ be a basis for P. g is completely determined by the mappings of e_i under g. Since f is an epimorphism, for every $g(e_i)$ in C, there exists $b_i \in B$ so that $f(b_i) = g(e_i)$. Define h by the basis mappings $e_i \mapsto b_i$.

Then $f \circ h = g$ as desired, since both g and $f \circ h$ are defined by the same basis mappings $e_i \mapsto b_i \mapsto f(b_i) = g(e_i)$.

B. P is R-projective $\iff$ $\exists Q$: R-module so $P \cup Q$ is R-free.

This seems equivalent to

(*) P is R-projective $\iff$ P is R-free.

If P is R-free, then $P \cup Q$ with $Q = 0$ is R-free, and if P is not P-free, then $P \cup Q$ for any Q is not R-free either; if $x \in P$ is a nonzero torsion elt., then so is $(x, 0)$ in $P \cup Q$. So I'll just show (*)

($\Leftarrow$): Part 2.

II.1B continued

($\Rightarrow$) I will show the equivalent statement

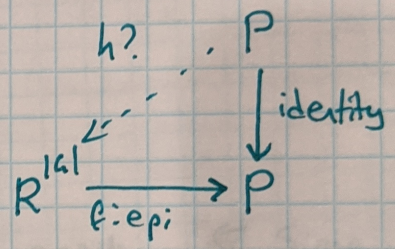
P is not R-free $\Rightarrow$ P is not R-projective.

Let $G = \{g_i\}$ be generators for P. Define an R-epi

$$f: R^{|G|} \to P$$

by basis mappings $e_i \mapsto g_i$ (e_i standard basis for $R^{|G|}$). This is well-defined as $\{e_i\}$ is a basis, and surjective since each generator is in the image of f.

Suppose that this commutativity diagram is given



If P were R-projective, then we should be able to find $h: P \to R^{|G|}$ R-homomorphism so that $f \circ h = id_P$. This is impossible.

Pick a nonzero torsion element $x \in P_t$, with nonzero $r \in R$ such that $rx = 0$. Then,

$$h(rx) = h(0) = r\,h(x) = 0 \in R^{|G|}$$

As $r \neq 0$ and $R^{|G|}$ is R-free, $h(x) = 0$. Then $f(h(x)) = 0 \neq x$, and $f \circ h \neq id_P$ for any $P \to R^{|G|}$ homomorphism h. So any non-R-free R-module is not R-projective.

II.2A. Let

$$0 \longrightarrow M' \xrightarrow{f:\text{mono}} M \xrightarrow{g:\text{epi}} M'' \longrightarrow 0$$

Be an exact sequence of R-modules. I claim

M is noetherian $\iff$ M' and M'' are noetherian.

($\Rightarrow$) Suppose M is noetherian. Then the submodule $\text{Im}(f) \subseteq M$ is noetherian as well (any ~~not-finitely-generated~~ submodule of $\text{Im}(f)$ is also a submodule of M and must be finitely generated).

Since f is a monomorphism, $M' \cong \text{Im}(f)$, and so M' is noetherian.

Now consider that

$$M \cong \ker(g) \amalg M/\ker(g)$$

$\ker(g) \cong M'$ as the sequence is exact. Since g is an epimorphism, $M/\ker(g) \cong M''$. So,

$$M \cong M' \amalg M'' \cong \ker(g) \overset{\amalg}{\oplus} M/\ker(g)$$

As M and M' are noetherian, so must M'' (consider that if M'' had an ∞-generated submodule N, then so would M — $0 \amalg N$ would be ∞-generated).

($\Leftarrow$). $M \cong M' \amalg M''$ as above. If M' and M'' are noetherian, then so is M.

Todo: II.2B, if I can.

III.1

Let V be a finite dimensional vector space and $T: V \to V$ a linear operator. Let V be an $F[t]$-module by

$$tv \mapsto T(v)$$

I claim that V is a finitely-generated torsion $F[t]$-module.

$\dim_F V$ is finite, so V is a f.g. F-module, and, as $F \subseteq F[t]$ (and the action of F on V as a $F[t]$-module is the same), V is a finitely-generated $F[t]$-module.

$F[t]$ is infinite dimensional over F, with basis $\{1, t, t^2 \ldots\}$. Meanwhile, End_F is finite-dimensional (consider that each has a finite matrix representation). So, the homomorphism $e_T: F[t] \to \mathrm{End}_F$ defined by evaluation at T is not injective.

Let $q_T \in \ker e_T$ be nonzero, monic, of minimal degree. This exists as $\ker e_T \neq 0$, well-ordering of $\mathbb{N}$ (degree), and since F is a field (allows scaling to monic polynomial).

Since $q_T(T) = 0$, for any $v \in V$,

$$q_T v \mapsto 0(v) = 0 \quad \text{with } q_T \neq 0$$

and V is a torsion $F[t]$-module.

II.2. Let V be fdvs over F (field?) of dimension n and let $T: V \to V$ be a linear operator.

A, T is triangularizable $\iff$ q_T factors as linear polynomials

($\Rightarrow$) Since T is triangularizable, there exists a basis $\mathcal{B}$ for which $[T]_{\mathcal{B}}$ is a triangular matrix. Compute the characteristic polynomial

$$f_T = \det(tI - [T]_{\mathcal{B}})$$

$tI - [T]_{\mathcal{B}}$ is a triangular matrix over $F[t]$. The determinant of a triangular matrix is the product of the diagonal entries, all of which are linear polynomials in this case. So f_T factors as linear polynomials.

f_T is the product of T's invariant factors. As q_T is an invariant factor, $q_T \mid f_T$, and, as $F[t]$ is Euclidean, and hence a UFD, q_T also factors as linear polynomials.

($\Leftarrow$) If q_T splits, then $JCF(T)$ exists. This is a triangularization of T.

B. If q_T splits with no repeated roots, then T is diagonalizable.

If q_T splits with no repeated roots, then all the elementary divisors of T are of multiplicity at most 1. So the Jordan blocks of T are all 1×1 and $JCF(T)$ is diagonal.

III.2.C

I believe $t^n - 2 \in \mathbb{Q}[t]$ is irreducible for all $n \geq 1$. (Pythagoras or someone proved this). Then $C(t^n - 2) =$

$$\begin{bmatrix} 0 & \cdots & 0 & +2 \\ 1 & 0 & & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & & 0 & \vdots \\ 0 & \cdots & 1 & 0 \end{bmatrix}$$

will define a linear operator on $\mathbb{Q}$ with $q_T = t^n - 2$ irreducible.

Ari.

III.3 Let $F = \mathbb{Z}_p$ ($= \mathbb{Z}/p\mathbb{Z}$) p: prime integer (is this what prime field is?)

Determine the RCF or JCF of all 3×3 matrices A with $A^4 = I$.

Since $A^4 = I$, we see that the minimal polynomial q_A must divide $t^4 - 1$. ($t^4 - 1 \in \operatorname{ann}_{F[t]} F^3$) with $tv \mapsto Av$

Case 1: $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = F$

In this case, $t^4 - 1$ splits as $(t-1)^4$

[the intermediate terms of the binomial expansion are even, hence 0 in $\mathbb{Z}_2$]

We can then have either $q_T = (t-1)$, or $q_T = (t-1)^2$, or ~~it is not possible for $q_T = (t-1)^2$~~ $q_T = (t-1)^3$.

This leads to these possible JCF (up to block order)

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

~~Case 1 ...~~

I believe this is the $p \equiv 1 \bmod 4$ case.

Case: $F = \mathbb{Z}/p\mathbb{Z}$; $p \geq 3$, and $t^4 - 1$ splits.

Let $t^4 - 1 = (t-1)(t+1)(t-A)(t+A)$ $[(t-A)(t+A) = t^2 + 1]$

Example: $\mathbb{Z}/5\mathbb{Z}$, $t^4 - 1 = (t-1)(t+1)(t-3)(t+3)$

For $p \geq 3$, $A \neq \pm 1$ [$t^2 + 1 \neq 0$ for $t = \pm 1$], and $A \neq -A$ as p is odd.

So all 4 roots are distinct. q_T divides $t^4 - 1$, so q_T also splits with no repeated roots. As shown in hw 9, this leads to a diagonal JCF $\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$ λ_i chosen from $\pm 1, \pm A$, possibly with repetition.

III.3 continued

Case: $F = \mathbb{Z}/p\mathbb{Z}$, $p \geq 3$ with t^2+1 irred. $p \equiv 3 \bmod 4$

$t^4 - 1 = (t-1)(t+1)(t^2+1)$

If $t^2+1 \nmid q_A$, then q_A splits without repetition, and the JCF(A) is $\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$ $\lambda_i \in \{\pm 1\}$ as before.

If $t^2+1 \mid q_A$, then q_A must be of degree 3. If q_A were of deg 2, then, ~~if~~ with or more $\cdots q_1 \mid q_2 = q_A$ being the invariant factors, we would have $f_A = q_1 q_2$ be degree at least 4, as q_2 is irred of deg 2.

Anyway, if $t^2+1 \mid q_A$, then q_A is degree 3 and either

$q_A = (t+1)(t^2+1)$ or

$q_A = (t-1)(t^2+1)$

and q_A is the only invariant factor. This leads to RCF(A) being

$\begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}$ or $\begin{bmatrix} 0 & 0 & +1 \\ 1 & 0 & -1 \\ 0 & 1 & +1 \end{bmatrix}$