Rings & Things

Fields and units.

- u is a *unit* if it has a multiplicative inverse, i.e., t such that $ut = 1$.
- A ring R is a *field* if every non-zero element is a unit.
- If an ideal contains a unit u then it is R itself, since it contains $(ru^{-1})u = r$ for all $r \in R$.

Integral Domains

- R is an *integral domain* (ID) if $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

For the rest of this sheet, assume we are in an ID.

Primes and irreducibles.

- p is *prime* if $p \,|\, ab \Rightarrow p \,|\, a$ or $p \,|\, b$.
- r is *irreducible* if $r = ab \Rightarrow$ one of a or b is a unit.
- Prime $\Rightarrow$ irreducible:

  Suppose $p = ab$. Then, since p is prime, $p \,|\, a$ or $p \,|\, b$. Suppose $p \,|\, a$, so that $a = pc$. Then $p = ab = pcb$, so $p(1 - cb) = 0$. As we are in an ID, either $p = 0$ or $cb = 1$. Thus b is unit.
- In general, irreducible $\not\Rightarrow$ prime.

  E.g., in $\mathbb{Z}[\sqrt{-6}]$, we have $6 = 2 \times 3 = (-\sqrt{-6})\sqrt{-6}$, with $2, 3, \sqrt{-6}$ all irreducible. So the irreducible 2 divides the product $(-\sqrt{-6})\sqrt{-6}$ but divides neither $\pm\sqrt{-6}$, so is not prime.

EDs, PIDs, UFDs.

- A *Euclidean function* is a map $\phi : R \to \mathbb{N}$ with one useful property being that if $a, b \in R, b \neq 0$ then there exist $q, r \in R$ such that $a = qb + r$ with $\phi(r) < \phi(b)$. It means we can apply a Euclidean algorithm, and ϕ gives a way of measuring whether the remainder is decreasing.

  E.g., $\phi(n) = |n|$ in the usual Euclidean algorithm on $\mathbb{Z}$, or $\phi(f) = \deg(f)$ for polynomials, or $\phi(z) = |z|^2$ for the Gaussian integers $\mathbb{Z}[i]$.
- R is a *Euclidean domain* (ED) if we can define such a Euclidean function.
- R is a *principal ideal domain* (PID) if every ideal is principal. That is, if $I \lhd R$ then $I = (r)$ for some $r \in R$. (Note that we can have a ring which is not an ID but in which every ideal is principal, such as $\mathbb{Z}/n\mathbb{Z}$ for composite n. Call this a *principal ideal ring*.)
- R is a *unique factorisation domain* (UFD) if each element can be uniquely factorised into irreducibles. (Unique up to order of factors and multiplication by units, that is.)

In an ED / PID / UFD, irreducible $\Rightarrow$ prime. (Proof in notes, I assume.)

Some implications.

Firstly, what do these imply about $R[X]$, the polynomial ring?

- R a field $\not\Rightarrow R[X]$ a field, since $1/X$ isn't a polynomial.

  R a field $\Rightarrow R[X]$ an ED, since we can take $\phi(f) = \deg(f)$ and do polynomial division.

  In fact, R a field $\Leftrightarrow R[X]$ a PID.

  ($\Rightarrow$) is because ED $\Rightarrow$ PID (see over the page).

  ($\Leftarrow$) Let $a \neq 0$. Then the ideal $(a, X) = (f)$ for some polynomial f (since we're in a PID), then $f \,|\, a$ (so $f =$ constant, since in an ID, $a = fg$ implies $\deg a = \deg f + \deg g$) and also $f \,|\, X$ (so $f =$ unit or $f =$ unit $\times X$). Thus $f =$ unit, and so $(f) = R$. So $1 \in (a, X)$, say $1 = ap(X) + Xq(X)$, so comparing coefficients gives $1 = ap_0$, i.e. a has an inverse.
- R an ED $\not\Rightarrow R[X]$ an ED, and R a PID $\not\Rightarrow R[X]$ a PID. For example, $\mathbb{Z}$ is a ED and PID, but in $\mathbb{Z}[X]$ the ideal $(2, X)$ is not principal. (And ED $\Rightarrow$ PID – see over the page.)
- R a UFD $\Rightarrow R[X]$ a UFD. Proof in notes, probably mentioning Gauss' lemma somewhere.
- R an ID $\Rightarrow R[X]$ an ID. Suppose $f(X) = \sum_{i=0}^{m} a_i X^i$, $g(X) = \sum_{i=0}^{n} b_i X^i$ with $a_m, b_n \neq 0$. Then $f(X)g(X) = a_m b_n X^{m+n} + \ldots$ with $a_m b_n \neq 0$. I.e., $f, g \neq 0 \Rightarrow fg \neq 0$.

Secondly, what do they imply about each other?

- Field $\Rightarrow$ the rest. Since every non-zero element is a unit:
  - If $b \neq 0$ then we can write $a = qb$ in the Euclidean algorithm, with $r = 0$. So it's an ED.
  - Any non-zero ideal contains a unit, so the only ideals are (0) and $R = (1)$. So it's a PID.
  - It's a UFD since factorisation up to units is done already.
  - If $ab = 0$ with $b \neq 0$ then multiplying by b^{-1} gives $a = 0$. So it's an ID.
- ED $\Rightarrow$ PID. If $I \triangleleft R$ with $I \neq \{0\}$, then take $b \in I$ with minimal ϕ value. If some $a \in I$ is not a multiple of b, then we can write $a = qb + r$ with $\phi(r) < \phi(b)$, contradiction. So $I = (b)$.

  Converse? PID $\not\Rightarrow$ ED, but this is hard to prove (so don't worry about it), as it requires showing that no Euclidean function exists. E.g., $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$.
- PID $\Rightarrow$ UFD. Proof in notes. (Idea: PID $\Rightarrow$ every element can be expressed as a product of irreducibles; PID $\Rightarrow$ irreducibles are prime; prime factorisation $\Rightarrow$ unique factorisation.)

  Converse? UFD $\not\Rightarrow$ PID (so not ED, field either). E.g., in $\mathbb{Z}[X]$, $(2, X)$ is not principal.
- UFD, PID, ED $\Rightarrow$ ID. That's what the 'D' means, so nothing to prove.

  Converse? ID $\not\Rightarrow$ UFD (so not PID, ED, field either). E.g., $\mathbb{Z}[\sqrt{-6}]$, as mentioned earlier.

Some other things.

- $P \triangleleft R$ is a *prime ideal* if $ab \in P \Rightarrow a \in P$ or $b \in P$. (Compare the definition of 'prime'.)
- P is a prime ideal if and only if R/P is an ID:

  R/P is an ID iff "$(a + P)(b + P) = ab + P = 0$ implies either $a + P = 0$ or $b + P = 0$" iff "$ab \in P$ implies either $a \in P$ or $b \in P$" iff P is prime.
- $M \triangleleft R$ is a *maximal ideal* if there is no ideal between it and R. That is, if for some ideal N we have $M \subseteq N \subseteq R$ then either $N = M$ or $N = R$.
- M is a maximal ideal if and only if R/M is a field:

  ($\Rightarrow$) Take $a + M \in R/M$ with $a \notin M$. Then the ideal $(a, M) \supsetneq M$, so it's R. So $1 \in (a, M)$, so $1 = \lambda a + m$ (some $\lambda \in R$, $m \in M$). Then in R/M, $(a + M)^{-1} = \lambda + M$, so R/M is a field.

  ($\Leftarrow$) Take $N \supsetneq M$, and $a \in N \setminus M$. In R/M, $a + M \neq 0$, so $(a + M)(b + M) = 1 + M$, some b, so $ab + M = 1 + M$, so $ab - 1 = m \in M$, so $1 = ab - m \in N$, so $N = R$, so M is maximal.
- Let R be a PID and α be an irreducible. Then (α) is a maximal ideal:

  If there is an ideal between (α) and R, it is principal, so we have $(\alpha) \subseteq (\beta) \subseteq R$, say. So $\beta \,|\, \alpha$, and so either β is a unit (in which case $(\beta) = R$) or $\beta = \text{unit} \times \alpha$ (in which case $(\beta) = (\alpha)$).

  Note that this doesn't follow in a non-PID. For example, 2 is irreducible in $\mathbb{Z}[X]$, but we have $(2) \subsetneq (2, X) \subsetneq \mathbb{Z}[X]$.

An example of how we can string all these together is to show that $\mathbb{F}_2[X]/(X^3 + X + 1)$ is a field.

> $\mathbb{F}_2$ is a field $\Rightarrow$ $\mathbb{F}_2[X]$ is a PID. In $\mathbb{F}_2$, the polynomial $X^3 + X + 1$ is irreducible (since if a cubic factorises then it must have a linear factor and thus a root, but 0 and 1 are the only elements in $\mathbb{F}_2$ and neither is a root), and so the ideal $(X^3 + X + 1)$ is maximal. Therefore the quotient $\mathbb{F}_2[X]/(X^3 + X + 1)$ is a field.

We have illustrated the following. We could include more arrows (e.g., horizontally in the second row), but these would make it more confusing (and most can be deduced from the rest anyway).