Ring Theory

- A field is a comm. ring F w/ identity $1 \neq 0$ in which every nonzero elt is a unit, i.e., $F^{\times} = F - \{0\}$.
- To check if subring, check ~~[illegible]~~ nonempty, closed under subtraction, and mult.
- Any finite integral domain is a field.
- The element $\alpha \in \mathcal{O}$ is a unit in $\mathcal{O}$ iff $N(\alpha) = \pm 1$.

Proposition: Let R be an int. dom. and let $p(x), q(x)$ be nonzero elts of $R[x]$. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$

(2) the units of $R[x]$ are just the units of R

(3) $R[x]$ is an integral domain.

- If S is a subring of R, then $S[x]$ is a subring of $R[x]$.

Definition: Let R and S be rings.

(1) A ring homomorphism is a map $\varphi: R \to S$ satisfying

  (i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ $\forall a, b \in R$

  (ii) $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in R$

(2) The kernel of the ring hom. φ, denoted $\ker(\varphi)$, is the set of elements of R that map to 0 in S.

(3) A bijective ring hom. is an isom.

Proposition: Let R and S be rings and let $\varphi: R \to S$ be a homomorphism.

(1) The image of φ is a subring of S

(2) The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker(\varphi)$, then $r\alpha$ and $\alpha r \in \ker(\varphi)$ $\forall r \in R$, i.e., $\ker(\varphi)$ is closed under mult. by elts. from R.

- The elt $b \in R$ belongs to the ideal (a) iff $b = ra$ for some $r \in R$, i.e., iff b is a multiple of a ~~non~~ ($a|b$ in R).
  ↳ $b \in (a)$ iff $(b) \subseteq (a)$.
- Let $m, n \in \mathbb{Z}^{+}$. $n\mathbb{Z} \subset m\mathbb{Z}$ iff $m|n$ in $\mathbb{Z}$

Example: we show that the ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal.

Observe that $(2, x) = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\}$ and so this ideal consists precisely of the polys. w/ $\mathbb{Z}$-coeffs whose constant term is even. In particular, this is a proper ideal. Assume by way of contradiction that $(2, x) = (a(x))$ for some $a(x) \in \mathbb{Z}[x]$. Since $2 \in (a(x))$ there must be some $p(x)$ s.t. $2 = p(x)a(x) \Rightarrow p, a$ must be constant polys. Since 2 is prime, $p, a \in \{\pm 1, \pm 2\}$. If $a(x) = \pm 1$, then every poly. would be a mult. of $a(x)$, contrary to $a(x)$ being a proper ideal. So $a(x) = \pm 2$. But now $x \in (a(x)) = (2) = (-2)$ and so $x = 2q(x)$ for some $q(x) \in \mathbb{Z}[x]$. $\lightning$ Therefore, $(2, x)$ is not principal.

- For any field F, all ideals of $F[x]$ are principal.

continued...

Proposition: Let I be an ideal of R.

(1) $I=R$ iff I contains a unit

(2) Assume R is comm. Then R is a field iff its only ideals are 0 and R.

Proof: (1) If $I=R$, then I contains the unit 1.
Conversely, if u is a unit in I with inverse v, then for any $r \in R$
$r = r \cdot 1 = r(uv) = r(vu) = (rv)u \in I$, hence $R = I$.

(2) The ring R is a field iff every nonzero elt. is a unit. If R is a field every nonzero ideal contains a unit, so by the first part R is the only nonzero ideal.
Conversely, if 0 and R are the only ideals of R, let u be any nonzero elt. of R. By hypothesis, $(u)=R$ and so $1 \in (u)$. Thus, there is some $v \in R$ s.t. $1 = vu$, i.e., u is a unit.
Every nonzero elt of R is therefore a unit and so R is a field.

Corollary: If R is a field, then any nonzero ring homomorphism from R into another ring is injective.

Definition: An ideal M in an arbitrary ring S is called a maximal ideal if $M \neq S$ and the only ideals containing M are M and S.

Proposition: In a ring w/ identity every proper ideal is contained in a maximal ideal.

Proof: Let R be a ring w/ id. and let I be a proper ideal (so R cannot be the zero ring). $1 \neq 0$
Let $\mathcal{S}$ be the set of all proper ideals of R that contain I. Then $\mathcal{S}$ is not empty ($I \in \mathcal{S}$) and is partially ordered by inclusion.
If $\mathcal{C}$ is a chain in $\mathcal{S}$, define J to be the union of all ideals in $\mathcal{C}$:
$J = \bigcup_{A \in \mathcal{C}} A$. We first show that J is an ideal.
Certainly, J is nonempty b/c $\mathcal{C} \neq \emptyset$. ($0 \in J$ since 0 is in every ideal A).
If $a, b \in J$, then there are ideals $A, B \in \mathcal{C}$ s.t. $a \in A$, $b \in B$. By definition of a chain either $A \subseteq B$ or $B \subseteq A$. In either case, $a-b \in J$, so J is closed under subtraction. Since each $A \in \mathcal{C}$ is closed under mult. by elts of R, so is J.
This proves J is an ideal.
If J is not a proper ideal, then $1 \in J$. In this case, by def. of J we must have $1 \in A$ for some $A \in \mathcal{C}$. ↯ b/c $A \in \mathcal{C} \subseteq \mathcal{S}$.
This proves that each chain has an upper bound in $\mathcal{S}$.
By Zorn's lemma, $\mathcal{S}$ has a maximal elt. which is therefore a maximal (proper) ideal containing I.

continued...

~~Proposition: Assume R is commutative. The ideal M is a maximal ideal iff the quotient ring R/M is a field.~~

<u>Definition</u>: Assume R is comm.. An ideal P is called a prime ideal if $P \neq R$ and whenever the product ab of two elts $a, b \in R$ is an elt of P, then at least one of a and b is an elt. of P.

- The prime ideals of $\mathbb{Z}$ are just the ideals $p\mathbb{Z}$ of $\mathbb{Z}$ generated by prime numbers p together w/ the ideal 0.

<u>Proposition</u>: Assume R is comm.. Then the ideal P is a prime ideal in R iff the quotient ring R/P is an integral domain.

<u>Proof</u>: The ideal P is prime $\Leftrightarrow$ $P \neq R$ and whenever $ab \in P$, then either $a \in P$ or $b \in P$.

use the bar notation for elts of R/P: $\bar{r} = r + P$

Note that $r \in P$ iff the elt $\bar{r}$ is zero in R/P.

Thus, P is a prime ideal $\Leftrightarrow$ $\bar{R} \neq \bar{0}$ and whenever $\overline{ab} = \bar{a}\bar{b} = \bar{0}$, then either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, i.e., R/P is an int. dom.

It follows ~~that~~ in particular that a comm. ring w/ identity is an int. dom. iff 0 is a prime ideal. $\square$

<u>Corollary</u>: Assume R is comm.. Every max ideal of R is a prime ideal.

<u>Proof</u>: If M is max. ideal, then R/M = field. A field is an int. dom. $\Rightarrow$ M is prime ideal. $\square$

<u>Proposition</u>: Assume R is comm. The ideal M is a maximal ideal iff R/M is a field.

<u>Proof</u>: $(\Rightarrow)$ Assume M is maximal. Then R/M is a comm. ring w/ identity. we have $R/M \neq 0$ since $R \neq M$. Therefore $1 \neq 0$ in R/M. Finally we check for inverses. Let $a+M$ be a nonzero elt of R/M. Then $a \notin M$ and we build a bigger ideal $I = \{ra + m : r \in R, m \in M\}$. (check that I is ideal). Since $a \in I$ and M is maximal, we must have $I = R$. But then $1 \in I$, so $1 = ra + m$ for some $r \in R$, $m \in M$. This means $1 + M = (r+M)(a+M)$. Since R/M is comm., this gives an inverse for $a+M$ and so R/M is a field.

$(\Leftarrow)$ Now assume R/M is field. Since $1 \neq 0$ in R/M, we have $M \neq R$. Assume there is an ideal I s.t. $M \subset I \subset R$. If $I \neq M$, let $a \in I$, $a \notin M$. Then $a+M$ has an inverse $u+M$ in R/M, so $au + M = 1 + M$. In particular, $au = 1 + m$ for some $m \in M$. Since $m \in M \subseteq I$, we have $1 = au - m \in I$ and so $I = R$. Therefore, M is maximal. $\square$

continued...

<u>Definition:</u> The ideals A and B of the ring R are said to be comaximal if $A+B=R$.

<u>Chinese Remainder Theorem:</u> Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map $R \to R/A_1 \times R/A_2 \times \ldots \times R/A_k$ defined by $r \mapsto (r+A_1, r+A_2, \ldots, r+A_k)$ is a ring hom. w/ kernel $A_1 \cap A_2 \cap \ldots \cap A_k$. If for each $i,j \in \{1,2,\ldots,k\}$ w/ $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \ldots \cap A_k = A_1 A_2 \ldots A_k$, so

$$R/(A_1A_2\ldots A_k) = R/(A_1 \cap A_2 \cap \ldots \cap A_k) \cong R/A_1 \times R/A_2 \times \ldots \times R/A_k.$$

<u>Proof:</u> We first prove this for $k=2$; the general case will follow by induction.
Let $A=A_1$ and $B=A_2$. Consider the map $\varphi: R \to R/A \times R/B$, defined by $\varphi(r) = \varphi(r \bmod A, r \bmod B)$, where mod A means the class in R/A containing r (that is, $r+A$).
This map is a ~~hom~~ ring hom. b/c φ is just the natural proj. ~~map~~ of R into R/A and R/B for the two components.
The kernel of φ consists of all the elts $r \in R$ that are in A and in B, i.e., $A \cap B$. To complete the proof in this case, it remains to show that when A and B are comaximal, φ is surj. and $A \cap B = AB$.
Since $A+B=R$, there are elts $x \in A$, $y \in B$ s.t. $x+y=1$.
This equation shows that $\varphi(x)=(0,1)$ and $\varphi(y)=(1,0)$ since for ex. $x \in A$ and $x = 1-y \in 1+B$.
If now $(r_1 \bmod A, r_2 \bmod B)$ is an arbitrary elt in $R/A \times R/B$, then the elts. $r_2x + r_1y$ maps to this elt. since

$$\begin{aligned}\varphi(r_2x+r_1y) &= \varphi(r_2x)+\varphi(r_1y) = \varphi(r_2)\varphi(x)+\varphi(r_1)\varphi(y) \\ &= (r_2 \bmod A, r_2 \bmod B)(0,1) + (r_1 \bmod A, r_1 \bmod B)(1,0) \\ &= (0, r_2 \bmod B) + (r_1 \bmod A, 0) = (r_1 \bmod A, r_2 \bmod B).\end{aligned}$$

This shows that φ is surj.
Finally, the ideal AB is always contained in $A \cap B$.
If A and B are comaximal and x,y are as above, then for any $c \in A \cap B$, $c = c1 = cx + cy \in AB$. This establishes $A \cap B \subseteq AB$, and completes the proof when $k=2$.

- $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$ as rings when $(m,n)=1$.

We also get $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

<u>Corollary:</u> Let $n \in \mathbb{Z}^+$ and $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = n$ into powers of distict primes. Then
$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$, as rings (same for $(\mathbb{Z}/n\mathbb{Z})^\times$ w/ unit gps.)

continued...

Proposition: Every ideal in a Euclidean domain is principal. More precisely, if I is any nonzero ideal in the Euclidean domain R, then $I=(d)$, where d is any nonzero elt of I of min. norm.

Proof: If $I=(0)$, there is nothing to prove.
Otherwise, let d be any nonzero elt of I of min. norm. (such a d exists since the set $\{N(a): a\in I\}$ has a minimum elt. by well-ordering of $\mathbb{Z}$).
Clearly $(d)\subseteq I$ since d is an elt. of I
To show $I\subseteq(d)$, let $a\in I$ and use the div. alg. to write $a=dq+r$ w/ $r=0$ or $N(r)<N(d)$. Then $r=a-qd$ and both $a, qd\in I \Rightarrow r\in I$.
By the minimality of the norm of d, we see that r must be 0.
Thus $a=qd\in(d) \Rightarrow I\subseteq(d)$.
Therefore, $I=(d)$. □

- Let $R=\mathbb{Z}[x]$. Since $(2,x)$ is not principal, $\mathbb{Z}[x]$ is not a Euclidean domain. (even though $\mathbb{Q}[x]$ is a Euclidean domain).

Example: Let $R=\mathbb{Z}[\sqrt{-5}]$, and consider $I=(3, 2+\sqrt{-5})$.
Suppose $I=(a+b\sqrt{-5})$, $a,b\in\mathbb{Z}$, were principal, i.e., $3=\alpha(a+b\sqrt{-5})$ and $2+\sqrt{-5}=\beta(a+b\sqrt{-5})$ for some $\alpha,\beta\in R$.
Taking norms we get $N(3)=9=N(\alpha)N(a+b\sqrt{-5})=N(\alpha)(a^2+5b^2)$
Since $a^2+5b^2>0$, we get that it must be $=1,3,$ or 9.
If $a^2+5b^2=9$, then $N(\alpha)=1$ and $\alpha=\pm1$, so $a+b\sqrt{-5}=\pm3$, which is impossible by the second equation since the coeffs. of $2+\sqrt{-5}$ are not divisible by 3.
The value cannot be 3 b/c there are no $\mathbb{Z}$-solns to $a^2+5b^2=3$.
If $a^2+5b^2=1$, then $a+b\sqrt{-5}=\pm1$ and $I=R$. But then $1\in I$, so $3\gamma+(2+\sqrt{-5})\delta=1$ for some $\gamma,\delta\in R$. Mult. both sides by $(2-\sqrt{-5})$ would imply that $2-\sqrt{-5}$ is a mult. of 3 in R, $\lightning$
Therefore, I is not principal $\Rightarrow$ R is not a Euclidean domain. □

- Note that $b|a$ in a ring R iff $a\in(b)$ iff $(a)\subseteq(b)$.
- $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID that is not a Euclidean domain.

Proposition: Every nonzero prime ideal in a PID is a maximal ideal.

Proof: Let (p) be a nonzero prime ideal in the PID R, and let $I=(m)$ be any ideal containing (p), so $(p)\subset(m)\subset R$. We WTS $I=(p)$ or $I=R$. Now $p\in(m)$, so $p=mr$ for some $r\in R$. Since (p) is a prime ideal and $rm\in(p)$, either $r\in(p)$ or $m\in(p)$. If $m\in(p)$, then $(m)=(p)=I$. If $r\in(p)$, then write $r=ps$. In this case $r=ps=r=(mr)s \Rightarrow sm=1$ (recall that R is an int. dom.) and m is a unit, so $(m)=R=I$. □

continued.

<u>Corollary</u>: If R is any comm. ring such that the poly. ring $R[x]$ is a PID (or a Euclidean domain), then R is necessarily a field.

<u>Proof</u>: Assume $R[x]$ is a PID. Since $R \subset R[x]$, then R must be int. domain (Recall that $R[x]$ has an id. iff R does).
The ideal (x) is a nonzero prime ideal in $R[x]$ because $R[x]/(x) \cong R$ which is an int. domain. Every nonzero prime ideal in a PID is a maximal ideal, so (x) is maximal. Hence $R[x]/(x) \cong R$ is a field. □

<u>Proposition</u>: In an integral domain a prime elt. is always irreducible.

<u>Proof</u>: Suppose (p) is a nonzero prime ideal and $p = ab$. Then $ab = p \in (p)$, so either $a \in (p)$ or $b \in (p)$. Say $a \in (p)$, then $a = pr$ for some r.
This implies $p = ab = prb \Rightarrow rb = 1$ and b is a unit. $\Rightarrow$ p is irred. □

- It is not true in general that an irred. elt. is necessarily prime.
Consider $3 \in \mathbb{Z}[\sqrt{-5}]$. 3 is irred. in $\mathbb{Z}[\sqrt{-5}]$, but 3 is not prime since $(2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$ is div. by 3, but neither $2+\sqrt{-5}$ or $2-\sqrt{-5}$ is div. by 3.

<u>Proposition</u>: In a PID a nonzero elt. is a prime $\Leftrightarrow$ it is irreducible.

<u>Proof</u>: Above we showed prime $\Rightarrow$ irred.
We must show conversely that if p is irred., then p is prime, i.e., the ideal (p) is prime.
If M is any ideal containing (p), then by hypothesis $M = (m)$ is a principal ideal.
Since $p \in (m)$, $p = mr$ for some $r \in R$. But p is irred. so either r or m is a unit. This means either $(p) = (m)$ or $(m) = (1)$.
Thus the only ideals containing (p) are (p) or (1), i.e., (p) is a maximal ideal. $\Rightarrow$ since we are in PID max ideal $\Rightarrow$ prime ideal. □

<u>Definition</u>: A UFD is an int. dom. R s.t. every nonzero elt $r \in R$, $r \neq$ unit has the following two properties:

(i) r can be written as a fin. prod. of irred. $p_i \in R$ (not nec. distinct) $r = p_1 p_2 \cdots p_n$ and

(ii) the decomp. in (i) is unique up to associates: namely, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irred, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \ldots, n$.

<u>Example</u>: $R[x]$ is a UFD whenever R is a UFD (in contrast to the properties of being a PID or Euclidean domain, which do not carry over from a ring R to the poly. ring $R[x]$.)

<u>Example</u>: $\mathbb{Z}[\sqrt{-5}]$ is not UFD b/c $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ ← 2 irred. factorizations.

continued...

Proposition: In a UFD a nonzero elt is a prime iff it is irreducible.

Proof: Let R be a UFD. Since a UFD is an int. domain and in an int. domain prime elts are always irred, it remains to show that each irred. elt is prime. Let p be an irred. elt. in R, and assume $p|ab$ for some $a,b \in R$. We WTS $p|a$ or $p|b$.

To say that $p|ab$ is to say $ab = pc$ for some $c \in R$.
Writing a and b as a product of irreducibles, we see from $ab = pc$ and from the uniqueness of the decomp. into irred. of ab, that the elt. p must be associate to one of the irred. occuring in either the factn of a or the factn of b.
WLOG assume p is associate to one of the irred. in the factn of a, i.e., a can be written as $a = (up)p_2 \cdots p_n$ for u a unit and some (possibly empty set of) irreducibles $p_2, \ldots, p_n$. But then p divides a, since $a = pd$ w/ $d = up_2 \cdots p_n$. $\square$

Theorem: Every PID is a UFD. In particular, every Euclidean dom. is a UFD.

- In $\mathbb{Z}[\sqrt{d}]$, if $N(\alpha) = \pm$ a prime (in $\mathbb{Z}$), then α is irred. in $\mathbb{Z}[\sqrt{d}]$.
- p factors in $\mathbb{Z}[i]$ into precisely two irred. iff $p = a^2 + b^2$ is the sum of two integer squares (otherwise p remains irred. in $\mathbb{Z}[i]$.).
- If $p \equiv 3 \mod 4$, then p is irred. in $\mathbb{Z}[i]$.

Proposition: The irred. ets of $\mathbb{Z}[i]$ are as follows:

(a) $1+i$ (norm = 2)
(b) the primes $p \in \mathbb{Z}$ with $p \equiv 3 \mod 4$ (which have norm p^2)
(c) $a+bi$, $a-bi$, the distinct irred. factors of $p = a^2+b^2 = (a+bi)(a-bi)$, for the primes $p \in \mathbb{Z}$ w/ $p \equiv 1 \mod 4$ (both of which have norm p).

Summary:

Fields $\subsetneq$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ integral domains (with all containments being proper.)

- $\mathbb{Z}$ is a Euclidean domain that is not a field
- $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID that is not a Euclidean domain
- $\mathbb{Z}[x]$ is a UFD that is not a PID
- $\mathbb{Z}[\sqrt{-5}]$ is an integral domain that is not a UFD.

Continued...

Proposition: Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polys w/ coeffs in I). Then $R[x]/(I) \cong (R/I)[x]$. In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$.

Proof: There is a natural map $\varphi: R[x] \to (R/I)[x]$ given by reducing each of the coefficients of a poly. mod. I.

The definition of add. and mult. in these two rings shows that φ is a ring hom.

The kernel is precisely the set of polynomials each of whose coeffs $\in I$, which $\ker(\varphi) = I[x] = (I)$, proving the first part of the prop.

The last statement follows from R int dom., then $R[x]$ int. dom.

Since if I is a prime ideal in R, then R/I is an integral domain, hence also $(R/I)[x]$ is an int. domain. This shows if I is prime in R, then (I) is prime in $R[x]$. $\square$

- Note that it's not true that if I is max. in R, then (I) is max. in $R[x]$. However, if I is maximal in R, then the ideal of $R[x]$ generated by I and x is maximal in $R[x]$.

Theorem: Let F be a field. The poly. ring $F[x]$ is a Euclidean domain. Specifically, if $a(x), b(x) \in F[x]$ with $b(x)$ nonzero, then there are unique $q(x), r(x) \in F[x]$ such that $a(x) = q(x)b(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.

Proof: If $a(x)$ is the zero polynomial, then take $q(x) = r(x) = 0$. We may therefore assume $a(x) \neq 0$, and prove the existence of $q(x), r(x)$ by induction on $n = \deg(a(x))$.

Let $b(x)$ have degree m. If $n < m$, take $q(x) = 0$ and $r(x) = a(x)$. Otherwise $n \geq m$. Write $a(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, and $b(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$.

Then the poly. $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ is of degree less than n (we have arranged to subtract the leading term from $a(x)$).

Note that this poly. is well defined b/c the coeffs are taken from a field and $b_m \neq 0$. By induction then, there exist polys $q'(x), r(x)$ with $a'(x) = q'(x)b(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.

Then, letting $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$ we have $a(x) = q(x)b(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$, completing the induction step.

- As for uniqueness, suppose $q_1(x), r_1(x)$ also satisfied the conditions of the thm. Then both $a(x) - q(x)b(x)$ and $a(x) - q_1(x)b(x)$ are of degree less than m ($m = \deg(b(x))$). The diff. of these two polys., i.e., $b(x)(q(x) - q_1(x))$ is also of degree $< m$. But the deg. of the product of two nonzero polys. is the sum of their degrees (since F is an int. dom.), hence $q(x) - q_1(x)$ must be 0, that is $q(x) = q_1(x)$. This implies $r(x) = r_1(x)$. $\square$

Corollary: If F is a field, then $F[x]$ is a PID and a UFD.

- If R is any comm. ring s.t. $R[x]$ is a PID (or Euclidean), then R must be a field.

Irreducibility Criteria

Proposition: Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree 1 iff $p(x)$ has a root in F, i.e., there is an $\alpha \in F$ w/ $p(\alpha)=0$.

Proof: If $p(x)$ has a factor of degree one, then since F is a field, we may assume the factor is monic, i.e., is of the form $(x-\alpha)$ for some $\alpha \in F$. But then $p(\alpha)=0$.

Conversely, suppose $p(\alpha)=0$. By the div. alg. in $F[x]$ we may write

$p(x) = q(x)(x-\alpha)+r$ where r is a constant.

Since $p(\alpha)=0$, r must be 0, hence $p(x)$ has $(x-\alpha)$ as a factor. $\square$

Proposition: A poly. of deg. 2 or 3 over a field F is red. $\Leftrightarrow$ it has a root in F.

Example: For p prime, the polys. x^2-p and x^3-p are irred. in $\mathbb{Q}[x]$.

Proposition: The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irred. polys. $f(x)$. In particular, $F[x]/(f(x))$ is a field $\Leftrightarrow$ $f(x)$ is irred.

Proposition: A finite subgp. of the mult. gp of a field is cyclic. In particular, if F is a finite field, then the mult. gp $F^\times$ of nonzero elts of F is a cyclic gp.

Proof: By the fund. thm. of fin. gen. abelian gps, the finite subgp can be written as a direct prod. of cyclic gps $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, where $n_k \mid n_{k-1} \mid n_{k-2} \mid \cdots \mid n_2 \mid n_1$. In general, if G is a cyclic gp and $d \mid |G|$, then G contains precisely d elts of order dividing d.

Since n_k divides the order of each cyclic gp in the direct prod., it follows that each direct factor contains n_k elts of order dividing n_k.

If k were greater than 1, there would therefore be a total of more than n_k such elts. But then there would be more than n_k roots of the poly. $x^{n_k}-1$ in the field F. $\lightning$ (a poly. of deg. n has at most n roots in F)

Hence $k=1$ and the gp is cyclic. $\square$

- $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, p prime.
- $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.