... multiplicity of $\sqrt{n}$. $\nexists$ $n \in \mathbb{N}$ and $\sqrt{n} \in \mathbb{Q}$, then $\exists$ $a, b \in \mathbb{N}$ $\ni$ $a/b = \sqrt{n}$. Squaring both sides, $N = a^2/b^2 = p_1^{2m_1} p_2^{2m_2}$ for some primes $p_1, p_2, \ldots p_k$. Since each prime has an even power, n is a □. Consequently if n is a non□ the $\sqrt{n} \notin \mathbb{Q}$ which shows $\sqrt{n}$ is irr.

Fundamental Theorem of Arith: Let $n \in \mathbb{N}$ then $\exists$ a unique set of distinct primes, $p_1, p_2, \ldots p_k$ and multiplicities $r_1, r_2, \ldots r_k$ for which $n = p_1^{r_1}, p_2^{r_2}, \ldots p_k^{r_k}$. Proof: If a prime divides the product of two natural #'s a,b, $n | ab$ then $p|a$ or $p|b$.

2□ identity: A sum of two squares times a sum of two squares is a sum of two squares.

PROOF: $(a_1^2+b_1^2)(a_2^2+b_2^2) = (a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2$

$= (a_1-b_1i)(a_1+b_1i)(a_2-b_2i)(a_2+b_2i)$

$= [a_1a_2-b_1b_2-(a_1b_2+b_1a_2)i] \times [a_1a_2-b_1b_2+(a_1b_2+b_1a_2)i]$

$= (a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2$

Prime Divisor Property: If a prime divides the product of natural numbers a and b, the p divides a or p divides b. Proof: $\nexists$ p does not divide a, so show p divides b. Now if p does not divide a, $\gcd(a,p)=1$, since only divisors of p are 1 and p. $\therefore$ $1 = ma+np$ for some $m,n \in \mathbb{Z}$ by linear representat of gcd. Multiplying both sides by b: $b = mab+npb$. $p|ab$ by assumption and $p|pb$. Thus $p|mab$ and npb. $\therefore p|(mab+npb)$

Divisibility Lemmas:

(i) If $a|b$ and $b|c$, then $a|c$. Proof: assume $a|b$ and $b|c$. Then $b=ak$ and $c=bj$ for some $j,k \in \mathbb{Z}$. Thus $c=akj$. Since $(kj) \in \mathbb{Z}$, $a|c$. (ii) If $a|b$ and $c|d$, then $ac|bd$. Proof: assume $a|b$ and $c|d$. Then $b=ak$ and $d=cj$ for some $j,k \in \mathbb{Z}$. $\therefore bd=(ak)(cj)=(ac)(kj)$ since $kj \in \mathbb{Z}$ $ac|bd$. (iii) $\nexists$ $m \neq 0$, then $ma|mb$ iff $a|b$. Proof: assume $ma|mb$. Then $mb = maj$ for some $j \in \mathbb{Z}$. Since $m \neq 0$, $\frac{1}{m}(mb) = \frac{1}{m}(maj) = b = aj$. Thus $a|b$. Now assume $a|b$. Then $b=ak$ f.s. $k \in \mathbb{Z}$. $mb = mak$. Since $(ak) \in \mathbb{Z}$, then $ma|mb$. (iv) If $d|a$ then $a=dj$ f.s. $j \in \mathbb{Z}$, $j \neq 0$. Thus $|dj| = |d||j| \Rightarrow |d||z|$ $\therefore$ $|a| = |d||j| \geq |d|$.

Fermat's lil thm: If p is prime and $a \not\equiv 0 \pmod p$, then $a^{p-1} \equiv 1 \bmod p$. Proof: $\mathbb{Z}/p\mathbb{Z}$ has p elements $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ has $p-1$. If $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ then by LaGrange's Thm $|H| \mid p-1$. Consider $H = \{a, a^2, \ldots, a^n = 1\}$ for $a \not\equiv 0 \pmod p$ & n is the least pwr for which $a^n \equiv 1 \bmod p$. $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$, so $|H| = n$ must divide $p-1$. $\therefore$ $p-1 = mn$ for some $m \in \mathbb{N}$. Thus $a^{p-1} = a^{mn}$ $= (a^n)^m \equiv 1^m \equiv 1 \bmod p$.

Wilson's Thm: If p is prime then $(p-1)! \equiv -1 \pmod p$. Proof: $1, 2, 3, \ldots p-1$ have inverses mod p. Consider $(p-1)! = (p-1)(p-2)\ldots 3, 2, 1$ which are order 2. $x^2 \equiv 1 \bmod p \Rightarrow x^2-1 \equiv (x-1)(x+1) \equiv 0 \bmod p \Rightarrow (x-1)(x+1)$ divided by p. But $a|b \Rightarrow p|a$ or $p|b$. Hence $p|x-1$ or $p|x+1$. $x \equiv 1$ or $x \equiv -1 \bmod p$.

Euler's Thm: If $[a]^{-1}$ exists for $\mathbb{Z}/n\mathbb{Z}$ then $a^{\varphi(k)} \equiv 1 \bmod k$. $|\mathbb{Z}/n\mathbb{Z}| = \#$ of elements $= \varphi(k) = |G \mapsto (\mathbb{Z}/n\mathbb{Z})^\times|$. $H = \{a, a^2, a^3 \ldots\} \leq G$ must be finite group, by LT, $|H| \mid |G| \Rightarrow$ least $n \ni a^n \equiv 1 \bmod n$ divides mod k

Unique Prime Factorization: Let $n \in \mathbb{N}$ then $\exists$ a unique set of distinct primes $p_1, p_2, \ldots p_k$ and multiplicities $r_1, r_2, \ldots r_k$ for which $n = p_1^{r_1}, p_2^{r_2} \ldots p_k^{r_k}$. proof: $\nexists$ $p_1 p_2 \ldots p_k$ $q_1 q_2 \ldots q_e$ where $p_i \neq q_j$ $\forall i,j$. Notice $p_1 | q_1(q_2 \ldots q_e)$ $\therefore p_1 | q_1$ or $p^1 | (q_2 \ldots q_e)$. $p_1 | q_1$ or $p_1 | q_2$ or $p_1 | q_e$ ...

$\gcd(a,b) | (ax+by)$ $\forall$ $x,y \in \mathbb{Z}$ $\therefore$ $\exists$ $x,y \ni ax+by=c$, then $\gcd(a,b)|c$. If $\gcd(a,b)|c$, then $[\gcd(a,b)]j = c$ f.s. $j \in \mathbb{Z}$. Also $\exists$ $m,n \in \mathbb{Z} \ni am+bn = \gcd(a,b)$. $c = \gcd(a,b)$ $= (am+bn)j = a(mj)+b(nj)$. $x = mj, y = nj$ gives $\mathbb{Z}$ solution to $ax+by=c$

Egyptian Fraction: $(20/13) = 1+(7/13) = (1+\frac{1}{2}+\frac{1}{26})$

Continued Fraction form: $\frac{99}{26} = 3+\frac{1}{(26/21)} = 3+\frac{1}{1+(5/21)}$ $= 3+\cfrac{1}{1+\cfrac{1}{(21/5)}} = 3+\cfrac{1}{1+\cfrac{1}{4+(1/5)}}$

THM Let d be □free & $d \neq n^2$ for some $n \in \mathbb{N}$ & $d \neq 0$, then $\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \mid a,b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{d}]$

Proof: Let $a,b,c,d \in \mathbb{Q}$ & $a \pm b, c \pm d \in \mathbb{Q}$

$(a+b\sqrt{d}) \pm (c+d\sqrt{d}) = a \pm c+(b \pm d)\sqrt{d} \in \mathbb{Q}\sqrt{d}$

$(a+b\sqrt{d})(c+d\sqrt{d}) = ac+bdd+(bc+ad)\sqrt{d} \in \mathbb{Q}\sqrt{d}$

If $z \in \mathbb{Q}\sqrt{d}$ w/ $z = x+y\sqrt{d} \neq 0$, then $\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{x-y\sqrt{d}}{x^2+dy^2}$ and $\frac{x}{x^2+dy^2}, \frac{-y}{x^2+dy^2} \in \mathbb{Q} \Rightarrow \frac{1}{z} \in \mathbb{Q}[\sqrt{d}]$. Since it is closed under $+, \times, \div$, $\mathbb{Q}\sqrt{d}$ is a field containing $\mathbb{Q}\sqrt{d}$ $\therefore$ $\frac{\mathbb{Q}\sqrt{d}}{\mathbb{Q}(\sqrt{d})}$

THE ONLY ALGEBRAIC $\mathbb{Z}$ INSIDE $\mathbb{Q}$ ARE ORDINARY $\mathbb{Z}$

Proof: Suppose $r = s/t$, $s,t \in \mathbb{Z}$ and $\gcd(s,t)=1$. Suppose r sat. the eq. $x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0 = 0$ where $a_0, a_1, \ldots a_{m-1} \in \mathbb{Z}$. Sub $\frac{s}{t}$ for x $\frac{s^m}{t^m} = -a_{m-1}\frac{s^{m-1}}{t^{m-1}} - \ldots - a_1\frac{s}{t} - a_0$. $s^m = -a_{m-1}s^{m-1}t - \ldots a_1st^{m-1} - a_0t^m$ $= (-a_{m-1}s^{m-1} - \ldots a_1s^{m-2} - a_0t^{m-1})t$

Since $\gcd(s,t)=1$ any prime factor of t ÷ RHS, but not LHS. $t = \pm 1$ by unique prime factorization in $\mathbb{Z}$, $\therefore$ r is an ordinary $\mathbb{Z}$

EQUIVALENT DEFN OF PRIME IDEALS

(1) $AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$ (2) $ab \in P \Rightarrow a \in P$ or $b \in P$

Proof: (1)$\Rightarrow$(2) $ab \in P \Rightarrow (ab) \subseteq P \Rightarrow (a)(b) \subseteq P \Rightarrow (a) \subseteq P$ or $(b) \subseteq P \Rightarrow a \in P$ or $b \in P$

(2)$\Rightarrow$(1) $\nexists$ $AB \subseteq P$ & $A \nsubseteq P$, show $B \subseteq P$. Since $A \nsubseteq P$, $\exists a \in A$ $\ni a \notin P$. $AB \subseteq P \Rightarrow ab \in P \Rightarrow a \in P$ or $b \in P$ $\Rightarrow b \in P$ by assumption $\Rightarrow B \subseteq P$.

$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if p is a square mod q} \\ -1 & \text{if p is not a square mod q} \end{cases}$

Quadratic Reciprocity:

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$; $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if $p,q = 4n+1$

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ otherwise

Suppliments:

$\left(\frac{-1}{q}\right) = 1 \Leftrightarrow q = 4n+1$

$\left(\frac{2}{q}\right) = 1 \Leftrightarrow q = 8n \pm 1$

Multiplicative Property of $\left(\frac{p}{q}\right)$

Proof: For any $p_1, p_2 \not\equiv 0 \pmod q$ $\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(\frac{p_1p_2}{q}\right)$

$\frac{p_1}{q} \equiv p_1^{\frac{q-1}{2}} \bmod q$ $\frac{p_2}{q} \equiv p_2^{\frac{q-1}{2}} \bmod q$

$\therefore \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) \equiv \left(p_1^{\frac{q-1}{2}}\right)\left(p_2^{\frac{q-1}{2}}\right) \bmod q$ $\equiv (p_1p_2)^{\frac{q-1}{2}} \bmod q \equiv \left(\frac{p_1p_2}{2}\right) \bmod q$

Unit: divisor of 1

RATIONAL NUMBERS ARE ONLY ALGEBRAIC #'S OF a ...

Proof: Let $\frac{a}{b} \in \mathbb{Q}$ be algebraic where $a,b \in \mathbb{Z}$. Since $P(x) = bx-a$ has $P(\frac{a}{b}) = b\frac{a}{b} - a = 0$. Also if α is degree 1 $\exists P(x) = a_1x+a_0 \ni P(\alpha) = a_1\alpha + a_0 = 0$ $\therefore \alpha = \frac{-a_0}{a_1} \in \mathbb{Q}$, by $a_1 \neq 0$.

MULTIPLICATIVITY OF NORM

$\alpha = a_1+b_1\sqrt{d}$ $\beta = a_2+b_2\sqrt{d}$

$\text{norm}(\alpha)\,\text{norm}(\beta) = \text{norm}(\alpha\beta)$

THM Given Ideals A, B of R the product AB is an ideal. Proof: Let $z, w \in AB$ and $r \in R$, then $\exists$ $a_j, b_j, c_j, d_j \in R$ where $a_j, c_j \in A$ & $b_j, d_j \in B$ for $j = 1, 2 \ldots h_1$ & $l = 1, 2 \ldots h_2$. WLOG $h = \max\{h_1, h_2\}$ assume $z = a_1b_1 + \ldots + a_nb_n$, $w = c_1d_1 + \ldots + c_nd_n$ where zero is added.

$z+w = a_1b_1 + c_1d_1 + \ldots + a_nb_n + c_nd_n \in AB$

$rz = ra_1b_1 + ra_2b_2 + \ldots + ra_nb_n \rightarrow ra \in A$

$= a'_1b_1 + a'_2b_1 + \ldots a'_nb_n \in AB$

$\therefore$ closed under add & mult

$\therefore$ AB is an ideal.

THM If I, J are ideals of R, I+J is an ideal of R

Proof: $\nexists$ I, J ideals of R. Consider $z_1, z_2 \in I+J$ and $r \in R$. $\exists x_1, x_2 \in I$ & $y_1, y_2 \in J \ni z_1 = x_1+y_1$, $z_2 = x_2+y_2$. $z_1+z_2 = (x_1+y_1)+(x_2+y_2) = (x_1+x_2)+(y_1+y_2)$ $= x_3+y_3$. As $x_1+x_2 = x_3 \in I$ and $y_1+y_2 = y_3 \in J$ since I, J are ideals. Thus $z_1+z_2 = x_3+y_3 \in I+J$

$rz_1 = r(x_1+y_1) = \underset{I}{rx_1} + \underset{J}{ry_1}$ $\therefore r_3 \in I+J$

PRINCIPAL IDEAL PROP. OF $\mathbb{Z}$

Proof: $\nexists$ I is an ideal of $\mathbb{Z}$ other than (0). Then I has a least mem, a. Since I is closed ×, I includes all members of $(a) = \{an : n \in \mathbb{Z}\}$. These are only mem of I, but if b is not a mult of a then b-(greatest mult of $a < b$) is pos mem of $I < a$, ✗.

MAXIMAL IDEALS ARE PRIME: Proof: $\nexists$ M is max ideal, $ab \in M$ and $a \notin M$. Show $b \in M$. $M[a] = \{ar+ms \mid r,s \in R, m \in M\}$ must be all of R. $1 \in M[a]$ so $\exists r,s \in R \ni 1 = ar+ms \Rightarrow b = bar+bms$. $bar \in M$, $m \in M \Rightarrow mbs \in M$ $\therefore b = bar + bms \in M$

MOD I FORMS EQ RELATION ON R

Proof: ① $a \equiv a \bmod I$ as $a-a = 0 \in I$ $\forall a \in R$

② $a \equiv b \bmod I \Rightarrow a-b \in I \Rightarrow b-a \in I \Rightarrow b \equiv a \bmod I$

③ $a \equiv b$ and $b \equiv c \bmod I \Rightarrow a-b \in I$, $b-c \in I$ hence $(a-b)+(b-c) = a-c \in I$ $\therefore a \equiv c \bmod I$

CHARACTERIZATION OF PRIME IDEALS

Proof: ⟹ $\nexists$ I is prime $(a+I)(b+I) = I \Rightarrow ab \in I \Rightarrow ab \in I \Rightarrow a \in I$ or $b \in I$ as I is prime $\Rightarrow R/I$ has no 0 divisors. ⟸ $\nexists$ R/I has no 0 divisors, show I is prime. $ab \in I \Rightarrow I+ab = I \Rightarrow (I+a)(I+b) = I$ $\Rightarrow I+a = I$ or $I+b = I$ since R/I has no zero div. $\Rightarrow a \in I$ or $b \in I$. $\Rightarrow$ I is a prime ideal.

THM: If R is the ring of integers for $\mathbb{Q}(\sqrt{d})$ and $d<0$, □free, then any ideal A has $A\bar{A} = (k)$ for some $k \in \mathbb{Z}$. [12.5]

R/I IS A RING W/RESPECT TO THE NAT. OP ON I+A. Proof: $(I+a)+(I+b) = I+(a+b)$ $= I+(b+a) = (I+b)+(I+a)$. $(I+a)+(I+a) = I = (a+a) = I+a = (I+a)+(I+0)$ Thus $I+0 = I$ plays role of 0 divisor.

THM If $I+A = I+a'$ and $I+b = I+b'$ then $I+(a+b) = I+(a'+b')$, $I+ab = I+a'b'$

Proof: $I+a = I+a'$, $I+b = I+b'$ $\Rightarrow a-a', b-b' \in I$. Thus $(a+b)-(a'+b') = (a-a')+(b-b') \in I$ closed under add. Also $ab-a'b' = ab+ab'-ab'-a'b' = a(b+b')-(a+a')b' = a(b-b')+(a-a')b'$ $\in I$

$\therefore ab-a'b' \in I$

CHARACTERIZATION OF MAX IDEALS: THM I is a max ideal of R, show R/I is a field. $I+a \neq I \Rightarrow a \notin I \Rightarrow J = \{i+ras \mid s \in R, i \in I\}$ an ideal must be $J = R \Rightarrow 1 = i+as$ for some $r, s \in R$ & $i \in I \Rightarrow I+as = I+1 \Rightarrow (I+a)(I+s) = I+1 \Rightarrow I+a$ has inverse $I+s$ $\Rightarrow$ R/I is a field.

12.5 CANCELLATION OF IDEALS: If A, B, C are nonzero ideals of R and $AB \supseteq AC$, $B \supseteq C$.

Proof: When $A = (\alpha)$ is principal. $AB \supseteq AC \Rightarrow (\alpha)A \supseteq (\alpha)B \Rightarrow \alpha B \supseteq \alpha C$. Since B and C are closed under × by mult of α, $(\alpha)B = \alpha B$ and $(\alpha)C = \alpha C \Rightarrow B \supseteq C$ × both sides by inverse. For general case, $AB \supseteq AC \Rightarrow \bar{A}AB \supseteq \bar{A}AC$ × both sides by $\bar{A}$ $\Rightarrow (k)B \supseteq (k)C$ for some $k \Rightarrow B \supseteq C$ by special case.

"CONTAINS MEANS DIVIDES" If A, B are ideals of R and $B \supseteq A$ then B divides A, $A = BC$ for some ideal C.

Proof: Special case where $B = (\beta)$ is a principal ideal. $B \supseteq A \Rightarrow (\beta) \supseteq A \Rightarrow \beta$ divides each mem of $A \Rightarrow A = (\beta)\{\alpha/\beta : \alpha \in A\} \Rightarrow A = BC$. In general case $B \supseteq A \Rightarrow B\bar{B} \supseteq A\bar{B}$ $\Rightarrow (k)\supseteq A\bar{B}$ (see 12.4) $\Rightarrow A\bar{B} = (k)C$ (for some ideal C, by special case) $\Rightarrow A\bar{B} = \bar{B}BC$ since $(k) = \bar{B}B$ $\Rightarrow A = BC$ by cancellation of ideal $\bar{B}$

EXISTENCE: Every nonzero ideal $A \neq R$ is product of prime ideals.

Proof: If A is not prime, then A is not maximal. $\exists$ ideal $B \ni A \subsetneq B \neq R$. $\exists$ C an ideal $\ni A = BC$ (since $B \supseteq A \Rightarrow B|A$). Then C is prime or we can factor it as above. Factoring at each step continues and at each step we absorb at least 1 element of form $I+R$, $\nexists$ finitely many $\supset I+r$.

UNIQUENESS: The factorization of a nonzero ideal is unique, up to the order of the factors.