Factorization in domains and zero-sum problems

B.Sury
Indian Statistical Institute Bangalore
National Mathematics Initiative
Conference on zero and related topics in number theory
IISc, July 26, 2016

Factorization problems in integral domains form an important aspect in commutative algebra.

Factorization problems in integral domains form an important aspect in commutative algebra.

An important class of domains more general than Dedekind domains is that of Krull domains; these are:

Factorization problems in integral domains form an important aspect in commutative algebra.

An important class of domains more general than Dedekind domains is that of Krull domains; these are:

Domains $R = \cap_{ht(P)=1} R_P$ where the localizations R_P at height 1 prime ideals are DVRs and each $a \neq 0$ in R belongs to at most a finite number of height one prime ideals.

Factorization problems in integral domains form an important aspect in commutative algebra.

An important class of domains more general than Dedekind domains is that of Krull domains; these are:

Domains $R = \cap_{ht(P)=1} R_P$ where the localizations R_P at height 1 prime ideals are DVRs and each $a \neq 0$ in R belongs to at most a finite number of height one prime ideals.

For Noetherian domains, this class coincides with the integrally closed ones.

Factorization problems in integral domains form an important aspect in commutative algebra.

An important class of domains more general than Dedekind domains is that of Krull domains; these are:

Domains $R = \cap_{ht(P)=1} R_P$ where the localizations R_P at height 1 prime ideals are DVRs and each $a \neq 0$ in R belongs to at most a finite number of height one prime ideals.

For Noetherian domains, this class coincides with the integrally closed ones.

In particular, Dedekind domains are Krull domains.

The starting point of this topic of factorization is the following beautiful result of Carlitz from 1960.

The starting point of this topic of factorization is the following beautiful result of Carlitz from 1960.

Theorem (Carlitz).
Let R be the ring of integers in an algebraic number field K. Then, K has class number ≤ 2 if, and only if, any two irreducible factorizations

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

in R have the same length ($r = s$).

The starting point of this topic of factorization is the following beautiful result of Carlitz from 1960.

Theorem (Carlitz).
Let R be the ring of integers in an algebraic number field K. Then, K has class number ≤ 2 if, and only if, any two irreducible factorizations

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

in R have the same length ($r = s$).

The integral domains with the above unique length property are now called half-factorial domains (HFDs).

Proof of Carlitz's theorem.
Suppose K has class number 2.

Proof of Carlitz's theorem.
Suppose K has class number 2.
Consider two irreducible factorizations

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Proof of Carlitz's theorem.
Suppose K has class number 2.
Consider two irreducible factorizations

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

We may assume that none of the p_i's and q_j's are primes.

Proof of Carlitz's theorem.
Suppose K has class number 2.
Consider two irreducible factorizations

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

We may assume that none of the p_i's and q_j's are primes.
Now, each (p_i) and each (q_j) is a product of two nonprincipal prime ideals; so, $2r = 2s$ and we have $r = s$.

For the converse, suppose R has class number > 2.

For the converse, suppose R has class number > 2.
If there exists an element $[P]$ of order $d > 2$, then writing $[P']$ for the inverse class, with P' prime, we get

$$P^d = (x), P'^d = (y), PP' = (z)$$

For the converse, suppose R has class number > 2.
If there exists an element $[P]$ of order $d > 2$, then writing $[P']$ for the inverse class, with P' prime, we get

$$P^d = (x), P'^d = (y), PP' = (z)$$

So $(xy) = (PP')^d = (z^d)$ which gives $xy = uz^d$ for some unit u. This expression shows R is not a HFD.

For the converse, suppose R has class number > 2.
If there exists an element $[P]$ of order $d > 2$, then writing $[P']$ for the inverse class, with P' prime, we get

$$P^d = (x), P'^d = (y), PP' = (z)$$

So $(xy) = (PP')^d = (z^d)$ which gives $xy = uz^d$ for some unit u. This expression shows R is not a HFD.
In case the class group is made of copies of $\mathbf{Z}_2$, look at elements $[P] \neq [Q]$.

For the converse, suppose R has class number > 2.
If there exists an element $[P]$ of order $d > 2$, then writing $[P']$ for the inverse class, with P' prime, we get

$$P^d = (x), P'^d = (y), PP' = (z)$$

So $(xy) = (PP')^d = (z^d)$ which gives $xy = uz^d$ for some unit u. This expression shows R is not a HFD.
In case the class group is made of copies of $\mathbf{Z}_2$, look at elements $[P] \neq [Q]$.
Then, $P^2 = (x), Q^2 = (y)$.

For the converse, suppose R has class number > 2.
If there exists an element $[P]$ of order $d > 2$, then writing $[P']$ for the inverse class, with P' prime, we get

$$P^d = (x), P'^d = (y), PP' = (z)$$

So $(xy) = (PP')^d = (z^d)$ which gives $xy = uz^d$ for some unit u. This expression shows R is not a HFD.
In case the class group is made of copies of $\mathbf{Z}_2$, look at elements $[P] \neq [Q]$.
Then, $P^2 = (x), Q^2 = (y)$.
If $[R]^{-1} = [P][Q]$ in the class group, write $PQR = (w)$.

For the converse, suppose R has class number > 2.
If there exists an element $[P]$ of order $d > 2$, then writing $[P']$ for the inverse class, with P' prime, we get

$$P^d = (x), P'^d = (y), PP' = (z)$$

So $(xy) = (PP')^d = (z^d)$ which gives $xy = uz^d$ for some unit u. This expression shows R is not a HFD.
In case the class group is made of copies of $\mathbf{Z}_2$, look at elements $[P] \neq [Q]$.
Then, $P^2 = (x), Q^2 = (y)$.
If $[R]^{-1} = [P][Q]$ in the class group, write $PQR = (w)$.
Now, if $R^2 = (z)$, we obtain $(w^2) = (xyz)$ which gives $w = uxyz$ for some unit u, again showing R is not a HFD.

It is important to note that the proof depends on the property that each nontrivial ideal class contains a prime ideal. This is NOT true for general Dedekind domains.

It is important to note that the proof depends on the property that each nontrivial ideal class contains a prime ideal. This is NOT true for general Dedekind domains.

HFDs need not be integrally closed; for example $\mathbf{Z}[\sqrt{-3}]$ is a HFD. In fact, we have the amazing:

The ring $\mathbf{Z}[\sqrt{-3}]$ is the unique, non- (integrally closed) order in an imaginary quadratic field which is a HFD.

The ring $\mathbf{Z}[\sqrt{-3}]$ is the unique, non- (integrally closed) order in an imaginary quadratic field which is a HFD.

Stark also proved an analogue of this class number one theorem:

The ring $\mathbf{Z}[\sqrt{-3}]$ is the unique, non- (integrally closed) order in an imaginary quadratic field which is a HFD.

Stark also proved an analogue of this class number one theorem:

The only imaginary quadratic fields whose rings of integers are HFDs are those with discriminants equal to:

The ring $\mathbf{Z}[\sqrt{-3}]$ is the unique, non- (integrally closed) order in an imaginary quadratic field which is a HFD.

Stark also proved an analogue of this class number one theorem:

The only imaginary quadratic fields whose rings of integers are HFDs are those with discriminants equal to:

$$-15, -20, -24, -35, -40, -51, -52, -88, -91, -115,$$

$$-123, -148, -187, -232, -235, -267, -403, -467.$$

The ring $\mathbf{Z}[\sqrt{-3}]$ is the unique, non- (integrally closed) order in an imaginary quadratic field which is a HFD.

Stark also proved an analogue of this class number one theorem:

The only imaginary quadratic fields whose rings of integers are HFDs are those with discriminants equal to:

$$-15, -20, -24, -35, -40, -51, -52, -88, -91, -115,$$

$$-123, -148, -187, -232, -235, -267, -403, -467.$$

As mentioned earlier, if we include orders, we need to add only the ring $\mathbf{Z}[\sqrt{-3}]$.

One has the following implication:

One has the following implication:

If an order R in an algebraic number field is a HFD, then so is its integral closure.

One has the following implication:

If an order R in an algebraic number field is a HFD, then so is its integral closure.

Later, we will give examples to show that this does not generalize to other domains.

One has the following implication:

If an order R in an algebraic number field is a HFD, then so is its integral closure.

Later, we will give examples to show that this does not generalize to other domains.

Also, analogous to Gauss's conjecture, one has:

One has the following implication:

If an order R in an algebraic number field is a HFD, then so is its integral closure.

Later, we will give examples to show that this does not generalize to other domains.

Also, analogous to Gauss's conjecture, one has:

Conjecture. There exist infinitely many real quadratic fields whose rings of integers are HFDs.

One has the following implication:

If an order R in an algebraic number field is a HFD, then so is its integral closure.

Later, we will give examples to show that this does not generalize to other domains.

Also, analogous to Gauss's conjecture, one has:

Conjecture. There exist infinitely many real quadratic fields whose rings of integers are HFDs.
In fact, one expects that there are infinitely many HFDs contained in $\mathbf{Z}[\sqrt{2}]$.

Claborn proved that every abelian group appears as the divisor class group of a Dedekind domain.

Claborn proved that every abelian group appears as the divisor class group of a Dedekind domain.

Zaks (who was the first to coin the phrase HFD) showed that the analogue of Carlitz's theorem is false in Dedekind domains in general.

Claborn proved that every abelian group appears as the divisor class group of a Dedekind domain.

Zaks (who was the first to coin the phrase HFD) showed that the analogue of Carlitz's theorem is false in Dedekind domains in general.

He showed in 1976:
Every finite abelian group occurs as the class group of a Dedekind HFD.

One may look at other types of extensions like polynomial rings over domains.

One may look at other types of extensions like polynomial rings over domains.

A natural question is whether the property that R is an HFD imply that $R[X]$ is an HFD; this turns out to be a subtle question.

One may look at other types of extensions like polynomial rings over domains.

A natural question is whether the property that R is an HFD imply that $R[X]$ is an HFD; this turns out to be a subtle question.

Coykendall proved the beautiful result:

Let R be any domain such that $R[X]$ is an HFD. Then, R must be integrally closed.

Let R be any domain such that $R[X]$ is an HFD. Then, R must be integrally closed.

In the same work, he also showed:

Let R be any domain such that $R[X]$ is an HFD. Then, R must be integrally closed.

In the same work, he also showed:
Let R be a Noetherian domnain. Then,

Let R be any domain such that $R[X]$ is an HFD. Then, R must be integrally closed.

In the same work, he also showed:
Let R be a Noetherian domnain. Then,
R is a Krull domain with class number ≤ 2 if, and only if,

Let R be any domain such that $R[X]$ is an HFD. Then, R must be integrally closed.

In the same work, he also showed:
Let R be a Noetherian domnain. Then,
R is a Krull domain with class number ≤ 2 if, and only if,
$R[X]$ is an HFD if, and only if,

Let R be any domain such that $R[X]$ is an HFD. Then, R must be integrally closed.

In the same work, he also showed:
Let R be a Noetherian domnain. Then,
R is a Krull domain with class number ≤ 2 if, and only if,
$R[X]$ is an HFD if, and only if,
$R[X_1, \cdots, X_n]$ is an HFD for all $n \geq 1$.

Let R be any domain such that $R[X]$ is an HFD. Then, R must be integrally closed.

In the same work, he also showed:
Let R be a Noetherian domnain. Then,
R is a Krull domain with class number ≤ 2 if, and only if,
$R[X]$ is an HFD if, and only if,
$R[X_1, \cdots, X_n]$ is an HFD for all $n \geq 1$.

In fact, Zaks's early work already shows the first statement implies the second because, if R is a Krull domain, then $R[X_1, \cdots, X_n]$ is also a Krull domain whose class group is the same.

Note that $\mathbf{Z}[\sqrt{-3}][X]$ is not a HFD by Coykendall's theorem.
In fact,

Note that $\mathbf{Z}[\sqrt{-3}][X]$ is not a HFD by Coykendall's theorem. In fact,

$$(2X + 1 + \sqrt{-3})(2X + 1 - \sqrt{-3}) = (2)(2)(X^2 + X + 1).$$

Note that $\mathbf{Z}[\sqrt{-3}][X]$ is not a HFD by Coykendall's theorem.
In fact,

$$(2X+1+\sqrt{-3})(2X+1-\sqrt{-3}) = (2)(2)(X^2+X+1).$$

Question. If R is a domain such that $R[X_1]$ is a HFD, is $R[X_1, X_]$ also a HFD?
The answer is yes if R is Noetherian.

The next natural question is if R is a domain such that $R[[X]]$ is a HFD, is it true that R is integrally closed?

The next natural question is if R is a domain such that $R[[X]]$ is a HFD, is it true that R is integrally closed?

This turns put to be false for $R = \mathbf{Z}[\sqrt{-3}]$. Thus, R is a HFD, $R[X]$ is not while $R[[X]]$ is!

The next natural question is if R is a domain such that $R[[X]]$ is a HFD, is it true that R is integrally closed?

This turns put to be false for $R = \mathbf{Z}[\sqrt{-3}]$. Thus, R is a HFD, $R[X]$ is not while $R[[X]]$ is!

We mentioned that if an order in a number field is a HFD, then so is its integral closure - this uses strongly that irreducibles in the integral closure can be thought of as irreducibles in the order, up to units.

The next natural question is if R is a domain such that $R[[X]]$ is a HFD, is it true that R is integrally closed?

This turns put to be false for $R = \mathbf{Z}[\sqrt{-3}]$. Thus, R is a HFD, $R[X]$ is not while $R[[X]]$ is!

We mentioned that if an order in a number field is a HFD, then so is its integral closure - this uses strongly that irreducibles in the integral closure can be thought of as irreducibles in the order, up to units.

Question. If a domain R is a HFD and its integral closure S is atomic, is S a HFD?

Just to recall, for a Krull domain R, the divisor class group is defined as follows.

Just to recall, for a Krull domain R, the divisor class group is defined as follows.
On non-zero fractional ideals, one defines the v-operation as $I_v = (I^{-1})^{-1}$.

Just to recall, for a Krull domain R, the divisor class group is defined as follows.
On non-zero fractional ideals, one defines the v-operation as $I_v = (I^{-1})^{-1}$.
Consider the set $div(R)$ of divisorial ideals (that is, non-zero fractional ideals I such that $I = I_v$.

Just to recall, for a Krull domain R, the divisor class group is defined as follows.
On non-zero fractional ideals, one defines the v-operation as $I_v = (I^{-1})^{-1}$.
Consider the set $div(R)$ of divisorial ideals (that is, non-zero fractional ideals I such that $I = I_v$.
The product of two divisorial ideals I, J may not be divisorial, but $(IJ)_v$ is divisorial; so, one defines the product of two elements I, J in $div(R)$ as $(IJ)_v$.

Just to recall, for a Krull domain R, the divisor class group is defined as follows.
On non-zero fractional ideals, one defines the v-operation as $I_v = (I^{-1})^{-1}$.
Consider the set $div(R)$ of divisorial ideals (that is, non-zero fractional ideals I such that $I = I_v$.
The product of two divisorial ideals I, J may not be divisorial, but $(IJ)_v$ is divisorial; so, one defines the product of two elements I, J in $div(R)$ as $(IJ)_v$.
The divisor class group is the quotient $div(R)/Prin(R)$ where $Prin(R)$ is the subgroup of all principal fractional ideals.

The most crucial property of Krull domains is the property that to every non-zero, non-unit $a \in R$, there are uniquely determined height one prime ideals $P_1, \cdots, P_n$ such that

$$aR = (P_1 \cdots P_n)_v.$$

The most crucial property of Krull domains is the property that to every non-zero, non-unit $a \in R$, there are uniquely determined height one prime ideals $P_1, \cdots, P_n$ such that

$$aR = (P_1 \cdots P_n)_v.$$

Decomposition of a non-zero, nonunit a into irreducibles corresponds to grouping the v-product of height one prime ideals into sub-v-products which do not admit any proper subproducts which are principal.

The most crucial property of Krull domains is the property that to every non-zero, non-unit $a \in R$, there are uniquely determined height one prime ideals $P_1, \cdots, P_n$ such that

$$aR = (P_1 \cdots P_n)_v.$$

Decomposition of a non-zero, nonunit a into irreducibles corresponds to grouping the v-product of height one prime ideals into sub-v-products which do not admit any proper subproducts which are principal.

That is, if $aR = (P_1 \cdots P_n)_v$ and $(P_1 \cdots P_r)_v = bR$ for some $r < n$, then there exists $c \in R$ such that $cR = (P_{r+1} \cdots P_n)_v$ and $a = bcu$ for some unit u.

For a Krull domain R, look at its class group $Cl(R)$ (written additively) and the subset S of non-zero classes which contain height one prime ideals.

For a Krull domain R, look at its class group $Cl(R)$ (written additively) and the subset S of non-zero classes which contain height one prime ideals.

We define a pair (G, S) with G an abelian group and S a subset of non-zero elements to be realizable, if there is a Krull domain R which realizes this pair as above.

For a Krull domain R, look at its class group $Cl(R)$ (written additively) and the subset S of non-zero classes which contain height one prime ideals.

We define a pair (G, S) with G an abelian group and S a subset of non-zero elements to be realizable, if there is a Krull domain R which realizes this pair as above.

(G, S) is realizable as above if, and only if, S generates G as a monoid.

In fact, we have the following refined version:

In fact, we have the following refined version:

Given a countably generated abelian group G and a nonempty subset S, there exists a Dedekind domain R with class group isomorphic to G with the additional property that the classes containing maximal ideals to constitute S if, and only if, S generates G as monoid.

In fact, we have the following refined version:

Given a countably generated abelian group G and a nonempty subset S, there exists a Dedekind domain R with class group isomorphic to G with the additional property that the classes containing maximal ideals to constitute S if, and only if, S generates G as monoid.

In particular, looking at $G = \mathbf{Z}_{k_1} \times \mathbf{Z}_{k_2} \times \cdots \mathbf{Z}_{k_n} \times \mathbf{Z}^r$ and $S = \{e_1, \cdots, e_n, e_{n+1}, \cdots, e_{n+r}, -e_{n+1}, \cdots, -e_{n+r}\}$, Zaks showed that there exists a Dedekind domain which is also a HFD such that its class group is isomorphic to any finitely generated abelian group.

In fact, we have the following refined version:

Given a countably generated abelian group G and a nonempty subset S, there exists a Dedekind domain R with class group isomorphic to G with the additional property that the classes containing maximal ideals to constitute S if, and only if, S generates G as monoid.

In particular, looking at $G = \mathbf{Z}_{k_1} \times \mathbf{Z}_{k_2} \times \cdots \mathbf{Z}_{k_n} \times \mathbf{Z}^r$ and $S = \{e_1, \cdots, e_n, e_{n+1}, \cdots, e_{n+r}, -e_{n+1}, \cdots, -e_{n+r}\}$, Zaks showed that there exists a Dedekind domain which is also a HFD such that its class group is isomorphic to any finitely generated abelian group.

It is known (due to Grams) that a pair (G, S) (where G is a finite abelian group G) is realizable if, and only if, S generates G as a group.

For a Krull domain R (which is not a UFD) and an irreducible, nonprime element $a \in R$, there exist unique height one prime ideals $P_1, \cdots, P_r$ whose v-product is the principal ideal (a); so, $\sum_{i=1}^{r} [P_i] = 0$ in $Cl(R)$. As a is irreducible, no proper subsum is 0 in $Cl(R)$.

For a Krull domain R (which is not a UFD) and an irreducible, nonprime element $a \in R$, there exist unique height one prime ideals $P_1, \cdots, P_r$ whose v-product is the principal ideal (a); so, $\sum_{i=1}^{r} [P_i] = 0$ in $Cl(R)$. As a is irreducible, no proper subsum is 0 in $Cl(R)$.

This prompted Davenport to come up with the following notion (now known as Davenport's constant):

For a Krull domain R (which is not a UFD) and an irreducible, nonprime element $a \in R$, there exist unique height one prime ideals $P_1, \cdots, P_r$ whose v-product is the principal ideal (a); so, $\sum_{i=1}^{r} [P_i] = 0$ in $Cl(R)$. As a is irreducible, no proper subsum is 0 in $Cl(R)$.

This prompted Davenport to come up with the following notion (now known as Davenport's constant):

Let G be a finite abelian group and $g_1, \cdots, g_r$ a sequence of elements whose sum is 0 and no proper subsum is 0. The Davenport constant of G is defined to be the largest such r (that is, largest r such that there is a sequence of length r with no proper subsequence summing to 0).

Given G, one may form a monoid $B(G)$ whose elements are "blocks" or sequences which sum to 0.

Given G, one may form a monoid $B(G)$ whose elements are "blocks" or sequences which sum to 0.
This is atomic if one looks at blocks which are irreducible (which means no proper subsum is 0).

Given G, one may form a monoid $B(G)$ whose elements are "blocks" or sequences which sum to 0.
This is atomic if one looks at blocks which are irreducible (which means no proper subsum is 0).
Given a subset S of nonzero elements in G, the monoid $B(G)$ has an atomic submonoid $B(S)$ whose elements are blocks built out of elements in S.

Given G, one may form a monoid $B(G)$ whose elements are "blocks" or sequences which sum to 0.
This is atomic if one looks at blocks which are irreducible (which means no proper subsum is 0).
Given a subset S of nonzero elements in G, the monoid $B(G)$ has an atomic submonoid $B(S)$ whose elements are blocks built out of elements in S.
Let R be Krull monoid with divisor class group G, and let S consist of those classes contain height one prime ideals. The map f which sends a nonzero element a in R to the block $[P_1], [P_2], \cdots, [P_r]$ where $P_1 \cdots P_r = aR$, is a length-preserving monoid homomorphism.

The Davenport constant of the class group plays a key role in the factorization theory of Krull domains but it is very hard to compute.

The Davenport constant of the class group plays a key role in the factorization theory of Krull domains but it is very hard to compute.

Olson was the first to study this in detail and determine the Davenport constants for some classes of groups.

The Davenport constant of the class group plays a key role in the factorization theory of Krull domains but it is very hard to compute.

Olson was the first to study this in detail and determine the Davenport constants for some classes of groups.

If $G = \mathbf{Z}_{n_1} \times \cdots \times \mathbf{Z}_{n_r}$ where $n_1 | n_2 | \cdots | n_r$, then one defines the number

$$M(G) = 1 + \sum_{i=1}^{r} (n_i - 1).$$

The Davenport constant of the class group plays a key role in the factorization theory of Krull domains but it is very hard to compute.

Olson was the first to study this in detail and determine the Davenport constants for some classes of groups.

If $G = \mathbf{Z}_{n_1} \times \cdots \times \mathbf{Z}_{n_r}$ where $n_1 | n_2 | \cdots | n_r$, then one defines the number

$$M(G) = 1 + \sum_{i=1}^{r} (n_i - 1).$$

It is easy to see that $D(G) \geq M(G)$.

It turns out that for groups of rank at most 2 (that is, $r = 1$ and $r = 2$), $D(G) = M(G)$.

It turns out that for groups of rank at most 2 (that is, $r = 1$ and $r = 2$), $D(G) = M(G)$.

This was conjectured to be always true - first conjectured for $\mathbf{Z}_p \times \mathbf{Z}_p$ by Erdős - but counter-examples were found later; the smallest counter-example is:

It turns out that for groups of rank at most 2 (that is, $r = 1$ and $r = 2$), $D(G) = M(G)$.

This was conjectured to be always true - first conjectured for $\mathbf{Z}_p \times \mathbf{Z}_p$ by Erdős - but counter-examples were found later; the smallest counter-example is:

Example. $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_6$ has $M(G) = 10$ and $D(G) > 10$.

The conjecture $D(G) = M(G)$ is still open for groups of rank 3 and rank 4 - equality has been proved in some cases.

The conjecture $D(G) = M(G)$ is still open for groups of rank 3 and rank 4 - equality has been proved in some cases.

Olson proved the equality $D(G) = M(G)$ for any p-group.

However, the general problem of determining $D(G)$ remains open and also determining which groups have $D(G) = M(G)$ is an interesting open question.

A natural method of evaluation of $D(G)$ is by employing group algebras - we shall use this to outline Olson's proof for p-groups.
Before that, let us define another interested notion.

A natural method of evaluation of $D(G)$ is by employing group algebras - we shall use this to outline Olson's proof for p-groups.
Before that, let us define another interested notion.

Given an atomic domain R, and any nonzero nonunit a, look at the supremum $\rho_R(a)$ of m/n where
$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ with p_i, q_j irreducible.

A natural method of evaluation of $D(G)$ is by employing group algebras - we shall use this to outline Olson's proof for p-groups.
Before that, let us define another interested notion.

Given an atomic domain R, and any nonzero nonunit a, look at the supremum $\rho_R(a)$ of m/n where
$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ with p_i, q_j irreducible.

One defines the elasticity $\rho(R)$ of R to be the supremum of $\rho_R(a)$ as a varies over nonzero nonunits.
HFDs have elasticity 1.

Narkiewicz proved for an algebraic number field K with nontrivial class group that $\rho(O_K) = D(Cl(K))/2$.

Narkiewicz proved for an algebraic number field K with nontrivial class group that $\rho(O_K) = D(Cl(K))/2$.

The proof works for any Dedekind domain with finite class group such that every ideal class contains a prime ideal.

Narkiewicz proved for an algebraic number field K with nontrivial class group that $\rho(O_K) = D(Cl(K))/2$.

The proof works for any Dedekind domain with finite class group such that every ideal class contains a prime ideal.
In fact, the result generalizes to Krull domains with nontrivial class group in which every nontrivial ideal class contains a height one prime ideal.

Apart from rings of integers which have finite elasticity by the above theorem, we also saw that the order $\mathbf{Z}[\sqrt{-3}]$ has elasticity 1.

Apart from rings of integers which have finite elasticity by the above theorem, we also saw that the order $\mathbf{Z}[\sqrt{-3}]$ has elasticity 1.

In contrast, in $\mathbf{Z}[\sqrt{-7}]$, for each $k \geq 2$, there is an element which is a product of $2k, 2k+1, \cdots, 3k$ irreducible elements at the same time!

Apart from rings of integers which have finite elasticity by the above theorem, we also saw that the order $\mathbf{Z}[\sqrt{-3}]$ has elasticity 1.

In contrast, in $\mathbf{Z}[\sqrt{-7}]$, for each $k \geq 2$, there is an element which is a product of $2k, 2k+1, \cdots, 3k$ irreducible elements at the same time!

Indeed, since $8 = (2)(2)(2) = (1-\sqrt{-7})(1+\sqrt{-7})$, we may raise them to the k-th power and keep replacing $(1-\sqrt{-7})(1+\sqrt{-7})$ by $(2)(2)(2)$.

Using norm maps, Coykendall has shown (and this is easy):

Using norm maps, Coykendall has shown (and this is easy):

If L/K is a Galois extension of algebraic number fields, and S is the monoid of integral norms from O_L to O_K, then $\rho(O_L) \geq \rho(S)$.

Using norm maps, Coykendall has shown (and this is easy):

If L/K is a Galois extension of algebraic number fields, and S is the monoid of integral norms from O_L to O_K, then $\rho(O_L) \geq \rho(S)$.
Further, if the norm of every irreducible element of O_L is irreducible in S, then $\rho(O_L) = \rho(S)$.

If $L = \mathbf{Q}(\sqrt{-14})$, one has $\rho(O_L) = 2$ because

$$(3)(3)(3)(3) = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}).$$

If $L = \mathbf{Q}(\sqrt{-14})$, one has $\rho(O_L) = 2$ because

$$(3)(3)(3)(3) = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}).$$

Note that $\rho(O_L) \leq D(Cl(O_L))/2 = 2$ from Narkiewicz's result also.

If $L = \mathbf{Q}(\sqrt{-14})$, one has $\rho(O_L) = 2$ because

$$(3)(3)(3)(3) = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}).$$

Note that $\rho(O_L) \leq D(Cl(O_L))/2 = 2$ from Narkiewicz's result also.

However, for the normset S with $K = \mathbf{Q}$, it can be shown that $\rho(S) = 3/2$ - note that 81 has elasticity 2 as an element but elasticity 1 as a norm.

Also, the above assertion $\rho(O_L) \geq \rho(S)$ is false in general for non-Galois extensions.

Also, the above assertion $\rho(O_L) \geq \rho(S)$ is false in general for non-Galois extensions.

For instance, if $L = \mathbf{Q}(\alpha)$ with $\min(\alpha, \mathbf{Q}) = X^5 - X^3 + 1$, it is known that O_L is a UFD (so $\rho(O_L) = 1$).

Also, the above assertion $\rho(O_L) \geq \rho(S)$ is false in general for non-Galois extensions.

For instance, if $L = \mathbf{Q}(\alpha)$ with $\min(\alpha, \mathbf{Q}) = X^5 - X^3 + 1$, it is known that O_L is a UFD (so $\rho(O_L) = 1$).

However,

$$3 = (\alpha^2 - \alpha - 1)(\alpha^4 - \alpha^3 - \alpha^2 - 1) = uv \ say$$

gives $N(u) = 3^2, N(v) = 3^3$ and hence $(3^3)^2 = (3^2)^3$ gives elasticity > 1 for S.

D.D.Anderson, D.F.Anderson and W.W.Smith have proved:

D.D.Anderson, D.F.Anderson and W.W.Smith have proved:

Any Krull domain R with finite, nontrivial divisor class group has rational elasticity m/n and there is an element admitting two irreducible factorizations of m, n.

D.D.Anderson, D.F.Anderson and W.W.Smith have proved:

Any Krull domain R with finite, nontrivial divisor class group has rational elasticity m/n and there is an element admitting two irreducible factorizations of m, n.

For an infinite field K, the domain $K[X^2, X^3]$ has infinite elasticity. If K is finite, then $\rho(K[X^2, X^3]) = 1 + D(K^+)/2$.

Other notions like cross number, and sets of lengths of elements have been studied with a view to characterizing the class group up to isomorphism. Further, the whole theory has widened in scope to include all Krull monoids.

Other notions like cross number, and sets of lengths of elements have been studied with a view to characterizing the class group up to isomorphism. Further, the whole theory has widened in scope to include all Krull monoids.

The cross number of a finite, abelian group G is defined to be

$$K(G) = exp(G) max\{\sum_{i=1}^{k} \frac{1}{|g_i|}\}$$

where $g_1, \cdots, g_k$ runs over minimal zero sum sequences.

Other notions like cross number, and sets of lengths of elements have been studied with a view to characterizing the class group up to isomorphism. Further, the whole theory has widened in scope to include all Krull monoids.

The cross number of a finite, abelian group G is defined to be

$$K(G) = exp(G)max\{\sum_{i=1}^{k} \frac{1}{|g_i|}\}$$

where $g_1, \cdots, g_k$ runs over minimal zero sum sequences.

Then, Krause showed:

Other notions like cross number, and sets of lengths of elements have been studied with a view to characterizing the class group up to isomorphism. Further, the whole theory has widened in scope to include all Krull monoids.

The cross number of a finite, abelian group G is defined to be

$$K(G) = exp(G) max\{\sum_{i=1}^{k} \frac{1}{|g_i|}\}$$

where $g_1, \cdots, g_k$ runs over minimal zero sum sequences.

Then, Krause showed:

The class group C of an algebraic number field is a cyclic group of prime power order if, and only if, the cross number $K(C) = exp(C)$.

Now, we outline a proof of Olson's theorem that for $G = \mathbf{Z}_{p^{e_1}} \times \cdots \times \mathbf{Z}_{p^{e_n}}$ we have $D(G) = 1 + \sum_{i=1}^{n}(p^{e_i} - 1)$. Call the RHS $M(G)$.

Now, we outline a proof of Olson's theorem that for $G = \mathbf{Z}_{p^{e_1}} \times \cdots \times \mathbf{Z}_{p^{e_n}}$ we have $D(G) = 1 + \sum_{i=1}^{n}(p^{e_i} - 1)$. Call the RHS $M(G)$.

Let us first observe $D(G) \geq M(G)$.

Now, we outline a proof of Olson's theorem that for $G = \mathbf{Z}_{p^{e_1}} \times \cdots \times \mathbf{Z}_{p^{e_n}}$ we have $D(G) = 1 + \sum_{i=1}^{n}(p^{e_i} - 1)$. Call the RHS $M(G)$.

Let us first observe $D(G) \geq M(G)$.

To see this, let $\{b_1, \cdots, b_n\}$ be a basis for G where b_i has order p^{e_i}.

Now, we outline a proof of Olson's theorem that for $G = \mathbf{Z}_{p^{e_1}} \times \cdots \times \mathbf{Z}_{p^{e_n}}$ we have $D(G) = 1 + \sum_{i=1}^{n}(p^{e_i} - 1)$. Call the RHS $M(G)$.

Let us first observe $D(G) \geq M(G)$.

To see this, let $\{b_1, \cdots, b_n\}$ be a basis for G where b_i has order p^{e_i}.

Consider the sequence where each b_i occurs $p^{e_i} - 1$ times; we can easily see that it is zero-sum free which gives us $D(G) \geq M(G)$.

The proof of $D(G) \leq M(G)$ uses the following observation:

The proof of $D(G) \leq M(G)$ uses the following observation:

Let $G = \mathbf{Z}_{p^{e_1}} \times \cdots \times \mathbf{Z}_{p^{e_n}}$ and let $g_1, \cdots, g_k$ be a sequence of elements in G such that $k \geq M(G)$. Then, $\prod_{i=1}^{k}(1 - g_i) = 0$ in the group ring $R_p := \mathbf{Z}_p[G]$.

Let $\{b_1, b_2, \cdots, b_n\}$ be a basis of G where order of b_i is p^{e_i}.

Let $\{b_1, b_2, \cdots, b_n\}$ be a basis of G where order of b_i is p^{e_i}. Since each g_j can be written as a product of the elements b_i, we can express $(1 - g_j)$ as a linear combination of the elements $1 - b_i$ with coefficients in R_p.

Let $\{b_1, b_2, \cdots, b_n\}$ be a basis of G where order of b_i is p^{e_i}. Since each g_j can be written as a product of the elements b_i, we can express $(1 - g_j)$ as a linear combination of the elements $1 - b_i$ with coefficients in R_p.
Thus,

$$(1 - g_1)(1 - g_2) \cdots (1 - g_k)$$

is a linear combination of the elements of the form $\prod_{i=1}^{n}(1 - b_i)^{a_i}$ where $\sum_{i=1}^{n} a_i = k > \sum_{i=1}^{n}(p^{e_i} - 1)$.

Let $\{b_1, b_2, \cdots, b_n\}$ be a basis of G where order of b_i is p^{e_i}.
Since each g_j can be written as a product of the elements b_i, we can express $(1 - g_j)$ as a linear combination of the elements $1 - b_i$ with coefficients in R_p.
Thus,

$$(1 - g_1)(1 - g_2) \cdots (1 - g_k)$$

is a linear combination of the elements of the form $\prod_{i=1}^{n}(1 - b_i)^{a_i}$ where $\sum_{i=1}^{n} a_i = k > \sum_{i=1}^{n}(p^{e_i} - 1)$.
Hence, there is at least one i such that $a_i \geq p^{e_i}$.

Let $\{b_1, b_2, \cdots, b_n\}$ be a basis of G where order of b_i is p^{e_i}. Since each g_j can be written as a product of the elements b_i, we can express $(1 - g_j)$ as a linear combination of the elements $1 - b_i$ with coefficients in R_p.
Thus,

$$(1 - g_1)(1 - g_2) \cdots (1 - g_k)$$

is a linear combination of the elements of the form $\prod_{i=1}^{n}(1 - b_i)^{a_i}$ where $\sum_{i=1}^{n} a_i = k > \sum_{i=1}^{n}(p^{e_i} - 1)$.
Hence, there is at least one i such that $a_i \geq p^{e_i}$.
In R_p, we therefore have $(1 - b_i)^{p^{e_i}} = 1 - b_i^{p^{e_i}} = 0$.

Using this observation, the proof is completed as follows.
Let $g_1, \cdots, g_k$ be an arbitrary sequence in G with $k \geq M(G)$.

Using this observation, the proof is completed as follows. Let $g_1, \cdots, g_k$ be an arbitrary sequence in G with $k \geq M(G)$. We show that $g_1, \cdots, g_k$ has a subsequence which sums to 0; this will show $D(G) \leq M(G)$ and hence we have equality.

Using this observation, the proof is completed as follows.
Let $g_1, \cdots, g_k$ be an arbitrary sequence in G with $k \geq M(G)$. We show that $g_1, \cdots, g_k$ has a subsequence which sums to 0; this will show $D(G) \leq M(G)$ and hence we have equality.
Now,

$$(1 - g_1) \cdots (1 - g_k) \equiv 0 \ mod \ p \cdots \cdots \cdots (\heartsuit)$$

Using this observation, the proof is completed as follows.
Let $g_1, \cdots, g_k$ be an arbitrary sequence in G with $k \geq M(G)$.
We show that $g_1, \cdots, g_k$ has a subsequence which sums to 0;
this will show $D(G) \leq M(G)$ and hence we have equality.
Now,

$$(1 - g_1) \cdots (1 - g_k) \equiv 0 \; mod \; p \cdots\cdots\cdots (\heartsuit)$$

We interpret this combinatorially.

For any $g \in G$, consider all subsequences of $g_1, \cdots, g_k$ which sum to g.

For any $g \in G$, consider all subsequences of $g_1, \cdots, g_k$ which sum to g.
Then, the coefficient of g in $(\heartsuit)$ equals $E(g) - O(g)$, where $E(g)$ (resp. $O(g)$) is the number of subsequences of even (resp. odd) length summing to g.

For any $g \in G$, consider all subsequences of $g_1, \cdots, g_k$ which sum to g.
Then, the coefficient of g in $(\heartsuit)$ equals $E(g) - O(g)$, where $E(g)$ (resp. $O(g)$) is the number of subsequences of even (resp. odd) length summing to g.
Clearly, from

$$(1-g_1)\cdots(1-g_k) \equiv 0 \ mod \ p \cdots\cdots\cdots(\heartsuit),$$

For any $g \in G$, consider all subsequences of $g_1, \cdots, g_k$ which sum to g.
Then, the coefficient of g in $(\heartsuit)$ equals $E(g) - O(g)$, where $E(g)$ (resp. $O(g)$) is the number of subsequences of even (resp. odd) length summing to g.
Clearly, from

$$(1 - g_1) \cdots (1 - g_k) \equiv 0 \ mod \ p \cdots\cdots\cdots (\heartsuit),$$

we have

$$E(0) - O(0) \equiv -1 \ mod \ p.$$

For any $g \in G$, consider all subsequences of $g_1, \cdots, g_k$ which sum to g.
Then, the coefficient of g in $(\heartsuit)$ equals $E(g) - O(g)$, where $E(g)$ (resp. $O(g)$) is the number of subsequences of even (resp. odd) length summing to g.
Clearly, from

$$(1 - g_1) \cdots (1 - g_k) \equiv 0 \ mod \ p \cdots\cdots\cdots (\heartsuit),$$

we have

$$E(0) - O(0) \equiv -1 \ mod \ p.$$

In particular, $E(0) - O(0) \neq 0$; so, there exists a subsequence of $g_1, \cdots, g_k$ which has sum 0. The proof is complete.

It was conjectured by Schinzel (and proved by Zakarczemny) that:

It was conjectured by Schinzel (and proved by Zakarczemny) that:

If G is a finite abelian group, and $g_1, \cdots, g_n \in G$, then the number of solutions of $\sum_{i=1}^n g_i x_i = 0$ in non-negative integers $x_i \leq c_i$ is at least $\frac{\prod_{i=1}^n (c_i+1)}{2^{d(G)-1}}$.

It was conjectured by Schinzel (and proved by Zakarczemny) that:

If G is a finite abelian group, and $g_1, \cdots, g_n \in G$, then the number of solutions of $\sum_{i=1}^{n} g_i x_i = 0$ in non-negative integers $x_i \leq c_i$ is at least $\frac{\prod_{i=1}^{n}(c_i+1)}{2^{d(G)-1}}$.

Zakarczemny later generalized the above result by showing that if $g \in G$ and $\sum_{i=1}^{n} g_i x_i = g$ admits a solution in non-negative integers $x_i \leq c_i$, then the number of such solutions is at least $\frac{\prod_{i=1}^{n}(c_i+1)}{3^{d(G)-1}}$.

It was conjectured by Schinzel (and proved by Zakarczemny) that:

If G is a finite abelian group, and $g_1, \cdots, g_n \in G$, then the number of solutions of $\sum_{i=1}^{n} g_i x_i = 0$ in non-negative integers $x_i \leq c_i$ is at least $\frac{\prod_{i=1}^{n}(c_i+1)}{2^{d(G)-1}}$.

Zakarczemny's proof is based on the polynomial identity (which is therefore valid in $\mathbf{Q}[G]$):

$$1 + t + t^2 + \cdots + t^n = \sum_{j=0}^{n} \frac{(1+t^j)(1+t)^{n-j}}{2^{n+1-j}}.$$

Zakarczemny later generalized the above result by showing that if $g \in G$ and $\sum_{i=1}^{n} g_i x_i = g$ admits a solution in non-negative integers $x_i \leq c_i$, then the number of such solutions is at least $\frac{\prod_{i=1}^{n}(c_i+1)}{3^{d(G)-1}}$.

Minimal lengths of zero-sum sequences with various other constraints have been widely studied starting form the Erdős-Ginzburg-Ziv theorem onwards. It is an active area of contemporary research.

Minimal lengths of zero-sum sequences with various other constraints have been widely studied starting form the Erdős-Ginzburg-Ziv theorem onwards. It is an active area of contemporary research.

The Erdős-Ginzburg-Ziv theorem asserts that any sequence of $2n - 1$ integers admits a subsequence of length n whose sum is $0 \bmod n$.

Minimal lengths of zero-sum sequences with various other constraints have been widely studied starting form the Erdős-Ginzburg-Ziv theorem onwards. It is an active area of contemporary research.

The Erdős-Ginzburg-Ziv theorem asserts that any sequence of $2n - 1$ integers admits a subsequence of length n whose sum is 0 mod n.

The EGZ theorem and the Davenport constant problem led people to introduce invariants that are important in zero-sum theory.

If G is a finite abelian group, define $\eta(G)$ to be the smallest integer l, such that every sequence of length at least l contains a zero-sum subsequence of length at most $exp(G)$; note $\eta(\mathbf{Z}_n) = n$.

If G is a finite abelian group, define $\eta(G)$ to be the smallest integer l, such that every sequence of length at least l contains a zero-sum subsequence of length at most $exp(G)$; note $\eta(\mathbf{Z}_n) = n$.

Define $s(G)$ to be the smallest integer l such that every sequence of length at least l has a zero-sum subsequence of length equal to $exp(G)$; note $s(\mathbf{Z}_n) = 2n - 1$.

If G is a finite abelian group, define $\eta(G)$ to be the smallest integer l, such that every sequence of length at least l contains a zero-sum subsequence of length at most $exp(G)$; note $\eta(\mathbf{Z}_n) = n$.

Define $s(G)$ to be the smallest integer l such that every sequence of length at least l has a zero-sum subsequence of length equal to $exp(G)$; note $s(\mathbf{Z}_n) = 2n - 1$.

It is easy to see $D(G) \leq \eta(G) \leq s(G) - exp(G) + 1$.

If G is a finite abelian group, define $\eta(G)$ to be the smallest integer l, such that every sequence of length at least l contains a zero-sum subsequence of length at most $exp(G)$; note $\eta(\mathbf{Z}_n) = n$.

Define $s(G)$ to be the smallest integer l such that every sequence of length at least l has a zero-sum subsequence of length equal to $exp(G)$; note $s(\mathbf{Z}_n) = 2n - 1$.

It is easy to see $D(G) \leq \eta(G) \leq s(G) - exp(G) + 1$.

Conjecture. $\eta(G) = s(G) - exp(G) + 1$.

If G is a finite abelian group, define $\eta(G)$ to be the smallest integer l, such that every sequence of length at least l contains a zero-sum subsequence of length at most $exp(G)$; note $\eta(\mathbf{Z}_n) = n$.

Define $s(G)$ to be the smallest integer l such that every sequence of length at least l has a zero-sum subsequence of length equal to $exp(G)$; note $s(\mathbf{Z}_n) = 2n - 1$.

It is easy to see $D(G) \leq \eta(G) \leq s(G) - exp(G) + 1$.

Conjecture. $\eta(G) = s(G) - exp(G) + 1$.

If one defines $E(G)$ to to be the analogue of $s(G)$ where $exp(G)$ is replaced by $|G|$, it can be shown that $D(G) = E(G) - |G| + 1$.

Finally, we mention that "weighted" zero-sum problems also arise naturally and many questions remain unresolved yet.

Finally, we mention that "weighted" zero-sum problems also arise naturally and many questions remain unresolved yet.

If G is a finite, abelian group and $S \subset G - \{0\}$, one may look at the variants $D_S(G), E_S(G)$ etc.

Finally, we mention that "weighted" zero-sum problems also arise naturally and many questions remain unresolved yet.

If G is a finite, abelian group and $S \subset G - \{0\}$, one may look at the variants $D_S(G), E_S(G)$ etc.

If G is $\mathbf{Z}_n$ and $S = \mathbf{Z}_n^*$, it can be shown that $E_S(G) = n + \omega(n)$.

Finally, we mention that "weighted" zero-sum problems also arise naturally and many questions remain unresolved yet.

If G is a finite, abelian group and $S \subset G - \{0\}$, one may look at the variants $D_S(G), E_S(G)$ etc.

If G is $\mathbf{Z}_n$ and $S = \mathbf{Z}_n^*$, it can be shown that $E_S(G) = n + \omega(n)$.

For a finite abelian group of order n, and any subset S consisting of non-zero elements, it is conjectured that $D_S(G) = E_S(G) - n + 1$ - this is not proved even for cyclic G.

As for the original Davenport constant, the best bound known in general is $D(G) \leq exp(G)\left(1 + \log\left(\frac{|G|}{exp(G)}\right)\right)$.

As for the original Davenport constant, the best bound known in general is $D(G) \leq exp(G)\left(1 + \log\left(\frac{|G|}{exp(G)}\right)\right)$.

This bound has been crucially used in the proof of infinitude of Carmichael numbers (in fact, to show that the number of these up to x is asymptotically at least $x^{2/7}$).

The proof of $D(G) \leq exp(G)\left(1 + \log\left(\frac{|G|}{exp(G)}\right)\right)$ goes as follows.

The proof of $D(G) \leq exp(G)\left(1+\log\left(\frac{|G|}{exp(G)}\right)\right)$ goes as follows.

Let $n \geq exp(G)\left(1+\log\left(\frac{|G|}{exp(G)}\right)\right)$ and $g_1, \cdots, g_n$ be a sequence of elements.

The proof of $D(G) \leq exp(G)\left(1 + \log\left(\frac{|G|}{exp(G)}\right)\right)$ goes as follows.

Let $n \geq exp(G)\left(1 + \log\left(\frac{|G|}{exp(G)}\right)\right)$ and $g_1, \cdots, g_n$ be a sequence of elements.

We fix a prime $p \equiv 1 \bmod exp(G)$ and show in the group algebra $\mathbf{F}_p[G]$ that for some elements $a_1, \cdots, a_n \in \mathbf{F}_p^*$, the product

$$(g_1 - a_1) \cdots (g_n - a_n) = 0.$$

The proof of $D(G) \leq exp(G)\left(1 + \log\left(\frac{|G|}{exp(G)}\right)\right)$ goes as follows.

Let $n \geq exp(G)\left(1 + \log\left(\frac{|G|}{exp(G)}\right)\right)$ and $g_1, \cdots, g_n$ be a sequence of elements.

We fix a prime $p \equiv 1 \bmod exp(G)$ and show in the group algebra $\mathbf{F}_p[G]$ that for some elements $a_1, \cdots, a_n \in \mathbf{F}_p^*$, the product

$$(g_1 - a_1) \cdots (g_n - a_n) = 0.$$

As $(g_1 - a_1) \cdots (g_n - a_n) = \sum_g c_g g$, if no subsequence of the g_i's has trivial product, then $c_1 = \prod_i (-a_i) \neq 0$, a contradiction.

To show $(g_1 - a_1)\cdots(g_n - a_n) = 0$, one shows that for each character $\chi \in \hat{G}$ (extended to the group algebra),

$$(\chi(g_1) - a_1)\cdots(\chi(g_n) - a_n) = 0.$$

To show $(g_1 - a_1)\cdots(g_n - a_n) = 0$, one shows that for each character $\chi \in \hat{G}$ (extended to the group algebra),

$$(\chi(g_1) - a_1)\cdots(\chi(g_n) - a_n) = 0.$$

One wishes to choose $a_1, \cdots, a_n \neq 0$ such that for each $\chi \in \hat{G}$, there is at least one i such that $\chi(g_i) = a_i$.

To show $(g_1 - a_1)\cdots(g_n - a_n) = 0$, one shows that for each character $\chi \in \hat{G}$ (extended to the group algebra),

$$(\chi(g_1) - a_1)\cdots(\chi(g_n) - a_n) = 0.$$

One wishes to choose $a_1, \cdots, a_n \neq 0$ such that for each $\chi \in \hat{G}$, there is at least one i such that $\chi(g_i) = a_i$.

This is accomplished by the greedy algorithm - that is, pick a_1 so that $\chi(g_1) = a_1$ for as many χ's as possible; pick a_2 so that $\chi(g_2) = a_2$ for as many of the remaining χ's as possible etc.

THANK YOU!