Today: divisibility properties.

Recall from number theory

Def $x \in \mathbb{C}$ is called algebraic integer if it satisfies a polynomial equation with integer coefficients and leading coefficient one, i.e.

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

$a_0, \ldots, a_{n-1} \in \mathbb{Z}$.

Properties:

1) $x \in \mathbb{Z} \Rightarrow x$ is alg. integer

Notation: $\overline{\mathbb{Z}}$ is the set of alg. integers.

$x \in \mathbb{Z} \Rightarrow x - a_0 = 0 \qquad a_0 = x \in \mathbb{Z}$

2) $x, y \in \overline{\mathbb{Z}} \Rightarrow x+y, \, xy \in \overline{\mathbb{Z}}$,

so $\overline{\mathbb{Z}}$ is a ring.

Idea of proof:

Let $x, y \in \overline{\mathbb{Z}}$

Write $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$

$y^m + b_{m-1}x^{m-1} + \ldots + b_0 = 0$

the corresponding equations.

Let $t^n + a_{n-1}t^{n-1} + \ldots + a_0 =$

$= \underline{(t-x_1)\ldots(t-x_n)}$

$t^m + b_{m-1}t^{m-1} + \ldots = (t-y_1)\ldots(t-y_m)$

Consider polynomials:

$$\prod_{\substack{i=1\\ j=1}}^{n,m} (t - x_i - y_j) = t^{mn} + p_{mn-1}t^{mn-1} + \ldots$$

$$\prod_{i=1}^{n}\prod_{j=1}^{m} (t - x_i y_j) = t^{mn} + q_{mn-1}t^{mn-1} + \ldots$$

Claim $p_k, q_k \in \mathbb{Z}$.

to prove it, in fact p_k, q_k are some polynomial expressions in $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1}$ with integer coefficients.

Consider x_i, y_i as variables.

Then p_k is some polynomial in $x_1, \ldots, x_n, y_1, \ldots, y_m$, which is invariant if we permute $x_1, \ldots, x_n$, also invariant if we permute $y_1, \ldots, y_m$.

Theorem if a polynomial in $x_1, \ldots, x_n$ is invariant under permutations, then it is a polynomial expression in the elementary symmetric polynomials = the coefficients $a_0, a_1, a_2, \ldots a_{n-1}$ of

$(t-x_1)\ldots(t-x_n) = t^n + a_{n-1}t^{n-1} + \ldots$ ∎

Example $x^2 + ax + b = 0$

$y^2 + cy + d = 0$

$(t-x_1)(t-x_2) = t^2 + at + b$

$a = -x_1 - x_2 \quad b = x_1 x_2$

$c = -y_1 - y_2 \quad d = y_1 y_2$

$(t - x_1 - y_1)(t - x_1 - y_2)(t - x_2 - y_1)(t - x_2 - y_2)$

$= t^4 + 2(a+c)t^3 + $

$\sum$ pairwise products $= \dfrac{\left(\sum_{i,j} x_i + y_j\right)^2 - \sum_{i,j}(x_i + y_j)^2}{}$

$= \dfrac{(2(a+c))^2 - 2(x_1^2 + x_2^2) - 2(y_1^2 + y_2^2) - 2(x_1 + x_2)(y_1 + y_2)}{2}$

$= 2(a+c)^2 - x_1^2 - x_2^2 - y_1^2 - y_2^2 - ac$

$= 2(a+c)^2 - a^2 + 2b - c^2 + 2d - ac$

$= a^2 + ac + c^2 + 2b + 2d$.

In general, very complicated expressions, but with integer coefficients.

For example $x = \dfrac{\sqrt{5}-1}{2} = 0{,}618\ldots$

$x^2 + x - 1 = 0 \quad \in \overline{\mathbb{Z}}$.

Property: $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.

Pf Let $\dfrac{m}{n} \in \overline{\mathbb{Z}} \quad (m,n) = 1 \quad n > 1$.

$m, n \in \mathbb{Z}$

$$\left(\frac{m}{n}\right)^k + a_{k-1}\left(\frac{m}{n}\right)^{k-1} + \ldots + a_0 = 0$$

$a_i \in \mathbb{Z}$

multiply by n^k, obtain

m^k is divisible by n, but $(m,n) = 1$ contradiction.

Main use of algebraic integers

if we want to prove $x \in \mathbb{Z}$, we can separately prove $x \in \mathbb{Q}$, $x \in \overline{\mathbb{Z}}$.

Let us look for algebraic integers in character theory.

Observation 1 if (V, ρ_V) is a representation of a finite group Γ, then $\forall g \in \Gamma$ $g^{|\Gamma|} = e$

$\rho_V(g)^{|\Gamma|} = e$, so for any eigenvalue λ of $\rho_V(g)$ satisfies $\lambda^{|\Gamma|} = 1 \Rightarrow \lambda$ is an algebraic integer. Hence $\chi_V(g) = \operatorname{tr} \rho_V(g)$ $=$ sum of eigenvalues $\in \overline{\mathbb{Z}}$.

So all entries of the character table are alg. integers.

Recall we want to prove $\dim V$ divides $|\Gamma|$ if V is irreducible, i.e. we want to prove

$$\underbrace{\frac{|\Gamma|}{\dim V}} \in \mathbb{Z}.$$

V is irreducible, we have

$$\sum_{g \in C} \rho_V(g) = \frac{|C|}{\dim V} \chi_V(g) \cdot Id_V.$$

Claim $\frac{|C|}{\dim V} \chi_V(g) \in \overline{\mathbb{Z}}$.

Pf: Consider instead of $\sum_{g \in C} \rho_V(g)$,

$\boxed{\sum_{g \in C} \rho_{\mathbb{C}[\Gamma]}(g)}$. This is a sum of permutation matrices,

so is a matrix with integer entries. Hence its characteristic polynomial has integer coefficients, so the eigenvalues are $\in \overline{\mathbb{Z}}$.

But $\frac{|C|}{\dim V} \chi_V(g)$ is one of the eigenvalues. (decomposing $\mathbb{C}[\Gamma]$ into irreducibles diagonalizes $\sum_{g \in C} \rho_{\mathbb{C}[\Gamma]}(g)$)

Consider $C_1, \dots, C_m$ conjugacy classes $g_i \in C_i$

$$\sum_{i=1}^{m} \underbrace{\frac{|C_i|}{\dim V} \chi_V(g_i)}_{\overline{\mathbb{Z}}} \cdot \underbrace{\chi_V(g_i^{-1})}_{\overline{\mathbb{Z}}} = \frac{|\Gamma|}{\dim V}$$

by orthogonality $\Rightarrow \frac{|\Gamma|}{\dim V} \in \overline{\mathbb{Z}} \Rightarrow$

$\frac{|\Gamma|}{\dim V} \in \mathbb{Z}$. ∎

Break until 10:48.

If eigenvalues are in $\overline{\mathbb{Z}}$ $\Rightarrow$ trace is in $\overline{\mathbb{Z}}$.

If moreover the matrix is scalar ($= \lambda \cdot Id$ $\lambda \in \mathbb{C}$) $\Rightarrow$ trace is divisible by the dimension.

Application of this property
($\dim V \mid |\Gamma|$).

Observation Γ is commutative if and only if it has only 1-dimensional irreducible representations.
Before we have seen:
Γ commutative $\Rightarrow$ Only 1-dimensional irreps.

to show $\Leftarrow$
we have $\rho_V(g)\rho_V(g') = \rho_V(g')\rho_V(g)$
$\forall g, g' \in \Gamma$, all irreducible V,
so also for all finite dimensional V.
So in particular for $V = \mathbb{C}[\Gamma]$.
so $gg' = g'g$ $\blacksquare$

Suppose $|\Gamma| = p^k$ p prime number
what is the smallest k such that Γ can be non commutative?

$k = 1$? $\Rightarrow$ Γ cyclic, hence commutative

$k = 2$? $\Rightarrow$ Γ is commutative.
Pf Γ is non-commutative $\Rightarrow$ has irrep of dim > 1, so $\geq p$.

$$p^2 + \underbrace{\dots}_{>0} = |\Gamma| = p^2$$

>0 because the trivial rep contributes 1.
contradiction.

$k = 3$? $|\Gamma| = p^3$
Ex 1 $p = 2$ $\square$-group
Ex 2 Heisenberg

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

$|H_p| = p^3$

affine

Quaternions group i, j, k,
$ij = k$ $i^2 = -1$, $j^2 = -1$, $k^2 = -1$
$(-1)^2 = 1$ -1 is in the center

$\#g$ s.t. g^2 is $\neq e$ central
for $\square$ this is 2
for quaternions this is 6.

dimensions of reps of H_p = ?
some have dim 1, some have dim p.

We can count reps of dim 1, then deduce how many have dim p. Homework.
Also compute char. table of quaternions.