Let R Ring R

new topic

Question: Why are the numbers always so nice? ($\chi(g)$)
They are always sums of roots of unity! So?

Def) A commutative ring R is \textit{Noetherian} if every ideal of R is finitely generated.

Def) Let R be a Noetherian ring, contained in some commutative ring T. An element $\alpha \in T$ is integral over R if $R[\alpha]$ is a finitely generated R-module.

ex Say $\frac{a}{b} \in \mathbb{Q}$ is a rat. number. If $\frac{a}{b} \in \mathbb{Z}$, then $\mathbb{Z}[\frac{a}{b}] = \mathbb{Z}$ is a 2013 11 18
finitely generated $\mathbb{Z}$-module so $\frac{a}{b}$ is integral over $\mathbb{Z}$.
Conversely, assume $\frac{a}{b} \notin \mathbb{Z}$. Then $\exists$ prime p st $p|b$, $p \nmid a$.
For any finite set $x_1, \dots, x_n \in \mathbb{Z}[\frac{a}{b}]$, there is some maximal power of p dividing the denominator of any x_i, so the $\mathbb{Z}$-module generated by $x_1, \dots, x_n$ cannot contain $\frac{a^m}{b^m}$ for m larger than that largest power.
So a rational number is integral over $\mathbb{Z} \Leftrightarrow$ it is an integer.

Theorem: Let $R \subseteq T$ be commutative rings, $\alpha \in T$. Then α is integral over R if and only if $\exists f(x) \in R[x]$ satisfying $f(\alpha) = 0$ and $f(x)$ is monic.
Proof: ($\Rightarrow$): Consider $\{1, \alpha, \alpha^2, \dots\} \subseteq R[\alpha]$. As $R[\alpha]$ is finitely generated, $\exists \{a_1, \dots, a_n\} \subseteq R[\alpha]$ st every $\gamma \in R[\alpha]$ can be written as $\gamma = r_1 a_1 + \dots + r_n a_n$ for some $r_i \in R$. But each a_i is a poly in α with coeffs in R. Let $N \in \mathbb{N}$ be bigger than the degree of each of these polynomials.
Then $\alpha^N = r_1 a_1 + \dots + r_n a_n$ for some $r_i \in R$. So $\alpha^N = f(\alpha)$ for some poly in R with degree less than N. Hence $x^N - f(x)$ is a monic poly with coeffs in R and α kills α.
($\Leftarrow$): Let $N = \deg(f)$. So $\alpha^N = r_{N-1}\alpha^{N-1} + \dots + r_0$. So $R[\alpha]$ is generated by $\{1, \dots, \alpha^{N-1}\}$ ∎

ex Which elements of $\mathbb{Q}(\sqrt{5})$ are integral over $\mathbb{Z}$?
What is the minimal poly of $\frac{a}{b}+\frac{c}{d}\sqrt{5} \in \mathbb{Q}(\sqrt{5})$? If $c=0$ we already know. Otherwise the min poly is

$$\left(x-\frac{a}{b}-\frac{c}{d}\sqrt{5}\right)\left(x-\frac{a}{b}+\frac{c}{d}\sqrt{5}\right) = x^2-\left(\frac{2a}{b}\right)x+\left(\frac{a^2d^2-5c^2b^2}{b^2d^2}\right).$$

When is this a poly with integer coeffs?
Well, $b \mid 2a$, $\gcd(a,b)=1 \Rightarrow b \mid 2$. So $b \in \{1,2\}$.
If $b=1$, then $d^2 \mid 5c^2 \Rightarrow d^2 \mid 5 \Rightarrow d=1$.
If $b=2$ then $4 \mid a^2d^2-5^2c^2 \Rightarrow 4 \mid a^2d^2 \Rightarrow 4 \mid d^2$ since a is odd. 2013 11 2
So $d=2d'$ for $d' \in \mathbb{Z}$.

So the integers of $\mathbb{Q}(\sqrt{5})$ are of the form $x+y\left(\frac{1+\sqrt{5}}{2}\right)$.

the set S of

Theorem: Let T be a commutative ring, $R \subseteq T$ a subring. If R, T are Noetherian then ~~the set~~ elements of T that are integral over R forms a subring of T.

Pf: Suffices to show S is non-empty and closed under $+, -, \cdot$. Well $R \subseteq S$, $R \neq \emptyset$. Let $x, y \in S$. Then $x+y, x-y, xy \in R[x,y]$, which is a finitely generated R-module, gen. by $\{x^i y^j\}$ where i, j range over the same sets as need to ensure that $\{x^i\}$ gen. $R[x]$, $\{y^j\}$ gen. $R[y]$.

Lemma: If R is Noetherian and M is a finitely gen. R-module, then every R-submodule of M is also fin. gen..

Pf: Say $N \subseteq M$ is an R-mod. Since M is gen. by $m_1, \dots, m_n$, $\exists$ surjective R-mod. hom $\phi: R^n \to M$ given by $\phi((r_1, \dots, r_n)) = r_1 m_1 + \cdots + r_n m_n$. If we can show that $\phi^{-1}(N)$ is a finitely gen R-mod. then N will also be fin gen, by the images (under ϕ) of the gen.s for $\phi^{-1}(N)$. Thus we may assume $M = R^n$. If $n = 1$, then N is an ideal of R, so is fin. gen. since R is Noetherian. Now proceed by ind. on n.

Define R-module hom $\pi: R^n \to R$ by $\pi(r_1, \dots, r_n) = r_1$. Then $\ker(\pi) \cong R^{n-1}$ is a finitely generated R-module and $\operatorname{im}(\pi)$ is also finitely generated because it's a submodule of R.

Furthermore, $\ker(\pi) \cap N$ is finitely generated because it's a submodule of R. Thus N can be finitely generated by the union of a set of generators for $\ker(\pi) \cap N$ and any finite set in N that maps (via π) to a finite generating set for $\operatorname{im}(\pi|_N)$. ∎

Hence if G is finite, χ any character, then $\chi(g)$ is integral over $\mathbb{Z}$ (as it is a sum of integral elements (roots of unity)) which form a ring.

2013 11 22

Theorem Let G be a finite group and $\rho: G \to GL(V)$ an irreducible representation. Then $\dim(V) \mid |G|$.

Proof: For any conjugacy class C of G, let

$$e_C = \sum_{g \in C} g \in \mathbb{C}[G].$$

Then e_C is in the centre of $\mathbb{C}[G]$, and $\bigoplus \mathbb{Z} e_C$ is a ring containing e_C that is a finitely generated $\mathbb{Z}$-module, so e_C is integral over $\mathbb{Z}$.

But $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$, and its centre is $\mathbb{C}\mathrm{Id} \times \cdots \times \mathbb{C}\mathrm{Id}$. The isomorphism maps $\Sigma a_i g_i$ to $(\Sigma a_i \rho_1(g_i), \ldots, \Sigma a_i \rho_r(g_i))$, where $\rho_i : G \to GL(V_i)$ is the i^{th} irred. representation (up to isomorphism).

So $\rho_i(e_C)$ is a scalar multiple of Id, meaning that $\frac{1}{\dim(V_i)} \mathrm{tr}(\rho_i(e_C))$ is integral over $\mathbb{Z}$. Thus, for any $\alpha = \Sigma a_i g_i$ in the centre of $\mathbb{C}[G]$, we have $\frac{1}{\dim(V)} \Sigma a_i \chi_\rho(g_i)$ is integral over $\mathbb{Z}$, for any character χ_ρ of any irreducible representation of G. Moreover, the span of $\{e_C\}$ is just the set $\{\Sigma f(g_i) g_i ;\ f \text{ is a class function}\}$.

So for any class function $f: G \to \mathbb{C}$, the sum $\frac{1}{\dim(V)} \Sigma f(g_i) \chi_\rho(g_i)$ is integral over $\mathbb{Z}$ for any irreducible representation.

If we choose $f(g_i) = \chi_\rho(g_i^{-1})$, then $\frac{1}{\dim(V)} \Sigma \chi_\rho(g_i^{-1}) \chi_\rho(g_i)$ is integral over $\mathbb{Z}$. But this sum is just $|G|/\dim(V) \in \mathbb{Q}$.

Thus $|G|/\dim(V) \in \mathbb{Z}$. ∎