Scratchwork: "Locally Compact Abelian" Groups

This harmonic analysis jargon "Locally Compact Abelian" groups appears basically all over number theory in a very abstract form. Here are the two examples I can think of immediately: $\mathbb{R}$ and $\mathbb{Q}_p$. Harmonic analysis is generalization of Fourier Analysis to abstract groups, such as $SO(3)$ the rotations of a three-dimensional object and many other kinds of symmetry.[1]

In our case, there is an isomorphism (as group) in Number Theory

$$\mathbb{Q}^\times = \prod_p p^{\mathbb{Z}} \quad \text{and} \quad \mathbb{Q}(i)^\times = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathbb{Z}}$$

In fact all the $F^\times$ are isomorphic for any number field F. That cannot be right. On the left the primes are $p \in \mathbb{Z}$ and on the right $\mathfrak{p} \in \mathbb{Z}[i]$ and for little more than grade school arithmetic, we have that primes $p \in 4\mathbb{Z}+1$ factor into $p = \mathfrak{p}_1\mathfrak{p}_2$ E.g. $13 = (2+3i) \times (2-3i)$ or $17 = (4+i) \times (4-i)$. Therefore both number fields share the primes in $p \in 4\mathbb{Z}+3$. So we need one extra thing to distinguish between $\mathbb{Q}^\times$ and $\mathbb{Q}(i)^\times$, that is a **topology**.

Have you seen Fourier analysis on $\mathbb{Q}^\times$ or $\mathbb{Q}(i)^\times$? These not compact, since we can find Cauchy sequences $x \to \sqrt{2}$ or $\sqrt{3} \notin \mathbb{Q}^\times$. So how can we define a derivative $f'(x) = 2x$.

$$f'(x) = \lim_{|\epsilon| \to} \frac{f(x+\epsilon) - f(x)}{\epsilon}$$

Therefore we need to find a space where this derivative makes any kind of sense at all. I think we have some freedom here. Why is this thing $f'(x)$ even a number?

Since I didn't study Munkres' textbook carefully (and all the pathological but nifty examples) we just settle for asking, which number $x \in \mathbb{Q}^\times$ or $x \in \mathbb{Q}(i)^\times$ solve $x \approx 0$? Which numbers are close to zero? And our number theory tool is called **strong approximation**. So there is in fact some ambiguity in the statement $x \to \sqrt{2}$ in a manner that is important to Number Theory.[2]

References

[1]

[1] When do we study a group action? Usually this means the object was not a priori symmetric! A cube can be rotated in three-dimensional space by $SO(3)$ elements, and we can study the remainder that's leftover.

[2] Don't just call their bluff, there should hopefully be a good reason.

01/24/19 One very easy "topological" group, or "Locally Compact Abelian" group should be $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, the rational numbers modulo the perfect squares. Why such a thing. Let's consider a variety of some kind:

$$V_1 = \{x^2 + y^2 = a\} \text{ and } V_2 = \{x^2 + y^2 = ab^2\}$$

The map $(x, y) \mapsto (bx, by)$ takes the small circle to the larger circle, so we call them *birational equivalent*.[3] So we can say that $V(a) \equiv V(ab^2)$ for $a, b \in \mathbb{Q}$. And more basically, $a \equiv ab^2$. Therefore our conic sections (mostly circles) are equivalence classes $[a] \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

What kind of observables can we study here? I'd like to count the rational points on this circle of a given height. For example:

$$\{x^2 + y^2 = 1\}$$

The rational points here correspond to **Pythagorian triples** or to **right triangles**. It's very unlikely that you've seen a proof of Pythagoras theorem. There are several hundred and they all say slightly different things about triangles. We would like the points in this circle of bounded height:

$$\left\{(a, b, c) \in \mathbb{Q} : \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \text{ and } |a|, |b|, |c| < N \text{ and } (a, b) = (a, c) = 1\right\}$$

We would have to "solve" the equation - and at this level it's harder and hard to means - and then we have to do GCD computations over and over. And we could let $f(N)$ be the number of points in this set.

Let's try one more. Here's a circle which clearly has points over $\mathbb{R}$ and yet is vacuous over $\mathbb{Q}$:

$$x^2 + y^2 = 3$$

No rational points whatsover. Since $\{0^2, 1^2\} + \{0^2, 1^2\} = \{0, 1, 2\}$ using a tiny amount of sumset theory. We've shown that $3 \notin \square$. We have shown a circle in $\mathbb{R}^2$ that has successfully avoided all of $\mathbb{Q}^2$. Nothing particularly wrong with that, but maybe we can quantify how close we can get to points in $\mathbb{Q}^2$.

As a temporary fix we could even completely solve this problem. We know that prime numbers split as the sum of two squares $p = a^2 + b^2$ iff $p = 4k + 1$. This is related to the field extension E/F with $E = \mathbb{Q}(i)^\times$ and $F = \mathbb{Q}$. We could study the two groups $E^\times/(E^\times)^2$ and $F^\times/(F^\times)^2$. We can even study $E^\times/F^\times = \mathbb{Q}(i)^\times/\mathbb{Q}^\times$. Our next helper is unique factorization.

$$\mathbb{Q}(i)^\times/\mathbb{Q}^\times \simeq \left(\prod_{p=4k+1} (p^{\mathbb{Z}} \oplus p^{\mathbb{Z}}) \times \prod_{p=4k+3} p^{\mathbb{Z}}\right) / \prod_p p^{\mathbb{Z}} \simeq \prod_{p=4k+1} p^{\mathbb{Z}}$$

And let's check that our perfect square group also has some kind of unique factorziation going on:

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \simeq \prod_p p^{\mathbb{Z}} / \prod_p p^{2\mathbb{Z}} \simeq \prod_p p^{\mathbb{Z}/2\mathbb{Z}}$$

We've had to pay several people off in order to get this wonderful reult:

- unique factorization of primes in $\mathbb{Z}$ and $\mathbb{Z}[i]$ and the GCD.
- Fermat's theorem $p = a^2 + b^2$ and Geometry of numbers or Dirichlet's Pigeonhole principle
- topology of numbers (uncharted territory). a few books on the topic in the bibliography

[3] Algebraic geometry is such that every time we make such a call, it merely becomes an invitation to check an endless hierarchy of exceptions. And it's OK. There are plenty of authoritive resources at varying levels.

The reason these are "topological groups" is that we need to decide when two of these numbers are "close" to each other in some sense. And these priems could get complicated too... can we stil run these objects into a compuer when $p = 4409$ or 6613? How about $p = 961,748,941$? And ike to tie into modern themes like **approximte groups** and **dynamical systems**.

Eventually these numbers are too big and we have to settle for approximate algorithms and estimates of runtimes. The very way we encode numbers into the computer will get called into question.

References

[1] Manfred Einsiedler, Thomas Ward. **Ergodic Theory with a view towards Number Theory** (Graduate Texts in Mathematics #259). Springer, 2011.

[2] Philippe Gille, Tamás Szamuely. **Central Simple Algebras and Galois Cohomology** (Cambridge Studies in Advanced Mathematics #165). Cambridge Uniersity Press, 2017.

[3] Pierre Guillot. **A Gentle Course in Local Class Field Theory** Cambridge University Press, 2018.

01/27/19 Let's try to write solutions to the sum of three squares as a "torus" orbit of some kind. The number $\sqrt{d}$ could be embedded into the quaternions. $\mathbb{Q}(\sqrt{n}) \to \mathbb{H}$. Let $a^2+b^2+c^2=n$, then $a\mathbf{i}+b\mathbf{j}+c\mathbf{k} \in \mathbb{H}$, with the correct norm. Then there is even a way to turn quaternions into 3×3 matrices. $\mathbb{Q}(\sqrt{n}) \to \mathbb{H} \to \mathsf{SO}(3)$.

1 $\mathbb{Q}(\sqrt{d})$ is an object where we adjoin the $\sqrt{d}$ to rationals. The example I usually give as to why these might be confusing objects:

$$\frac{a}{b}+\frac{c}{d}\sqrt{d} = \frac{a+b\sqrt{d}}{c+d\sqrt{d}} = \frac{(a+b\sqrt{d})(c-d\sqrt{d})}{c^2-d\,d^2}$$

Let's try type-setting this correctly.

$$\frac{a}{b}+\frac{c}{d}\sqrt{m} = \frac{a+b\sqrt{m}}{c+d\sqrt{m}} = \frac{(a+b\sqrt{m})(c-d\sqrt{m})}{c^2-m\,d^2}$$

That formula can't possibly be right, but it can be fixed. Here's another example. Since $\sqrt{d} \in \mathbb{R}$ is a real number,

$$\overline{\mathbb{Q}} = \mathbb{R} \text{ but also } \overline{\mathbb{Q}(\sqrt{d})} = \mathbb{R} \text{ and even } \overline{\mathbb{Q}} = \mathbb{Q}_p \text{ for all primes } p \in \mathbb{Z}$$

$\mathbb{R}$ could be thought of as the "completion" of $\mathbb{Q}$ at the prime $p=\infty$. We'd have $\mathbb{R}=\mathbb{Q}_\infty$. The field $\mathbb{Q}(\sqrt{d})$ is even worse since it has *two* infinite places.

$$|a+b\sqrt{d}|_1 = |a+b\sqrt{d}| \in \mathbb{R} \text{ and } |a+b\sqrt{d}|_2 = |a-b\sqrt{d}| \in \mathbb{R}$$

In fact it's customary to plot them in a grid according to two different sets of projections either:

$$a+b\sqrt{d} \to (a,b) \in \mathbb{Q}^2 \subseteq \mathbb{R}^2 \text{ or } (a+b\sqrt{d}, a-b\sqrt{d}) \in \mathbb{R}^2$$

No surprises there either. The second grid is useful when we want to find that $\mathbb{Z}[\sqrt{d}]^\times$ is cyclic.[4]

We have that the completion $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ could be $\mathbb{Q}_p$ or $\mathbb{R}=\mathbb{Q}_\infty$ depending on our choice of "norm". Tricky but not surprises there either. Are we OK that $|15|_5 = \frac{1}{5}$ and yet $|15|_\infty = |15|$?

2 Todays surprise is that we can embed $\mathbb{Q}(\sqrt{d})^\times \to \mathbb{H}^\times$ as a multiplicative subset of the quaternions.

$$\begin{aligned} 1 &\mapsto 1 \\ \sqrt{m} &\mapsto a\,\mathbf{i}+b\,\mathbf{j}+c\,\mathbf{k} \text{ for } a^2+b^2+c^2=m \end{aligned}$$

And I know of a standard way to turn quaternions into either 2×2 complex matrices or 3×3 real matrices. First:

$$a_0+a_1\,i+a_2\,j+a_3\,k \mapsto \begin{bmatrix} a_0+a_1\,\mathbf{i} & a_2+a_3\,\mathbf{i} \\ -a_2+a_3\,\mathbf{i} & a_0-a_1\,\mathbf{i} \end{bmatrix}$$

with the additional integer constraint that $a_1^2+a_2^2+a_3^2=m$.

Then we turn into a rotation. I get this formula from Wikipedia:

$$a_0+a_1\,i+a_2\,j+a_3\,k \mapsto \begin{bmatrix} a_0^2+a_1^2-a_2^2-a_3^2 & 2(a_1a_2-a_0a_3) & 2(a_0a_2+a_1a_3) \\ -2(a_1a_2-a_0a_3) & a_0^2-a_1^2+a_2^2-a_3^2 & 2(a_2a_3-a_0a_1) \\ -2(a_0a_2+a_1a_3) & -2(a_2a_3-a_0a_1) & a_0^2-a_1^2-a_2^2+a_3^2 \end{bmatrix} \in \mathsf{SO}_3(\mathbb{R})$$

[4]That is not technically true, it depends on $d \in \mathbb{Z}$. [**not technically true**] $\notin [true, false]$ It's not always true that $\mathcal{O}(\mathbb{Q}(\sqrt{d})) \simeq \mathbb{Z}[\sqrt{d}]$. It's only true about half the time, and . Unique factorization in $\mathbb{Q}(\sqrt{d})$ and in $\mathbb{Q}(\sqrt{-d})$ always fails for $D > 100$.

This is a lot of information to keep track of. $\mathbb{R}$ has already uncountable infinite elements, and such commplexity, so how can we understand the rotation group?

Everything here is **more or less**.

- 20 minutes more or less
- 5 inches more or less.
- 150 kilograms more or less.

None of these exotic topologies really matter. Just $\mathbb{R}$ or the faux $\mathbb{R}$ that we're using on our cash registers and calculators. Perhaps we could start to theorize about the spaces we are measuing. We could define a map $\mu : X \to \mathbb{R}$. For any reasonable subset $X \subseteq \mathbb{R}$. Here X is just the thing we are measuring and μ is the subset. What could go wrong with that?