Group theory helped win World War II

In the 1920's, Poland felt threatened by its neighbor Germany. In order to determine Germany's intent, the Poles monitored German radio transmissions. Beginning in 1928, the Poles ran into a roadblock decrypting the German messages and began to suspect that the Germans were using a machine cipher. The Germans had begun using Enigma. In 1932, Polish Intelligence recruited three mathematicians to attack the Enigma cipher. One of these mathematicians Marian Rejewski was able to use group theory to exploit patterns in German messages; he was able to determine the wiring of the rotors and the rotor settings. Until 1938 . We will look at how Rejewski used group theory to determine the settings of the Enigma rotors. .