# Two theorems of Glaisher and Kaplansky

David Brink

October 2008

**Abstract**. We give a new proof of a recent theorem of Kaplansky and use it to revive an old, seemingly forgotten result of Glaisher.

It is well known that, for any $n > 0$, the prime numbers of the form $x^2 + ny^2$ can be described by congruence conditions if and only if $n$ is one of Euler's *convenient numbers* [4, p. 62]. Since 1, 2, 4, 8 and 16 are the only convenient powers of 2, the following theorem of Kaplansky [8] is remarkable: *A prime $p \equiv 1$ (mod 16) is representable by both or none of $x^2+32y^2$ and $x^2+64y^2$, whereas a prime $p \equiv 9$ (mod 16) is representable by exactly one of these forms.* Kaplansky writes, "Although this is a simple elementary statement I do not have a direct proof. Instead I shall show that it is a quick corollary of two significant theorems." The latter are reciprocity laws concerning 2 and –4 as fourth and eighth power residues. In this note we give a new proof of Kaplansky's theorem that aspires to be direct. Instead of reciprocity it uses an idea of Aigner [1], Barrucand and Cohn [2], namely that both representations $p = u^2 + v^2$ and $p = z^2 + 2w^2$ of a prime $p \equiv 1 \pmod 8$ come from a single representation of $p$ by the norm form of the eighth cyclotomic field.

Consider an odd prime $p$ and let $h$ and $h'$ be the class numbers corresponding to the discriminants $-4p$ and $-8p$, respectively. Using Kaplansky's theorem, we give a quick proof of an old, seemingly forgotten result of Glaisher[1]: *If $p \equiv 1$ (mod 16), then either both or none of $h$ and $h'$ are divisible by 8; if $p \equiv 9$ (mod 16), then exactly one of these class numbers is divisible by 8.* This was originally demonstrated in [5, §12] along with other interesting class number relations using Dirichlet's class number formula.

*Proof of Kaplansky's theorem.* Consider a prime $p \equiv 1 \pmod 8$. It splits in the eighth cyclotomic field $\mathbb{Q}(\zeta)$, $\zeta^4 + 1 = 0$. Therefore, and since the ring of integers $\mathbb{Z}[\zeta]$ is a PID, $p$ is the norm of an integer $a + b\zeta + c\zeta^2 + d\zeta^3$, i.e. $p = a^4 + b^4 + c^4 + d^4 + 2a^2c^2 + 2b^2d^2 + 4a^2bd - 4ab^2c - 4bc^2d + 4acd^2$ with $a, b, c, d \in \mathbb{Z}$. Now $u = a^2 - c^2 + 2bd$, $v = d^2 - b^2 + 2ac$, $z = a^2 - b^2 + c^2 - d^2$ and $w = ab + cd + ad - bc$ satisfy the identities

$$p = u^2 + v^2 = z^2 + 2w^2 \qquad (*)$$

[1] James W. L. Glaisher (1848–1928), son of the meteorologist and world record holding balloonist of the same name.

where $u$ may be assumed odd. Then $v \equiv 0 \pmod 4$, $w \equiv 0 \pmod 2$, and $u, v, z, w$ are all unique modulo sign. One sees immediately from $(*)$ that the conditions

(1a) $u \equiv \pm 1 \pmod 8$
(1b) $z + 2w \equiv \pm 1 \pmod 8$
(1c) $p \equiv 1 \pmod{16}$

are equivalent. Since $u$ is odd, $a$ and $c$ must have different parity. Hence it follows from $v + z = (a + c)^2 - 2b^2 \equiv \pm 1 \pmod 8$ that

(2a) $v \equiv 0 \pmod 8$
(2b) $z \equiv \pm 1 \pmod 8$

are equivalent. Combining this with the above gives that also

(3a) $u + v \equiv \pm 1 \pmod 8$
(3b) $w \equiv 0 \pmod 4$

are equivalent, a fact also contained in [2, Main Theorem]. Finally, it is clear that either all three or only one of (1a), (2a) and (3a) holds. Consequently, either all three or only one of (1c), (2a) and (3b) holds, which concludes the proof. □

*Proof of Glaisher's theorem.* It is an immediate consequence of the Gaussian theory of genera that $2 \mid h$ if and only if $p \equiv 1 \pmod 4$, and that always $2 \mid h'$. Glaisher showed that $4 \mid h$ if and only if $p \equiv 1 \pmod 8$, and that $4 \mid h'$ if and only if $p \equiv \pm 1 \pmod 8$. Furthermore, $8 \mid h$ if and only if $p$ is of the form $x^2 + 32y^2$, and $8 \mid h'$ if and only if $p$ is either of the form $x^2 + 64y^2$ or $\equiv -1 \pmod{16}$. The first of these two beautiful theorems was proved by Barrucand and Cohn and later, in a different manner, by Hasse [6]. The second was proved for $p \equiv -1 \pmod 8$ by Glaisher and for all $p$ by Hasse [7][2]. Glaisher's and Kaplansky's theorems are now seen to follow from one another. □

Five results similar to Kaplansky's theorem were found in [3], for example the following: *A prime $p \equiv 1$ (mod 20) is representable by both or none of $x^2 + 20y^2$ and $x^2 + 100y^2$, whereas a prime $p \equiv 9$ (mod 20) is representable by exactly one of these forms.* The proof used class field theory. As a final remark, we give here a different, more elementary demonstration using the same basic idea as above: Consider a prime $p \equiv 1, 9 \pmod{20}$. It splits in the field $\mathbb{Q}(\sqrt{5}, i) = \mathbb{Q}(\alpha)$ where $\alpha^4 + 3\alpha^2 + 1 = 0$. Since the ring of integers $\mathbb{Z}[\alpha]$ is a PID, $p$ is the norm of an integer $a + b\alpha + c\alpha^2 + d\alpha^3$, i.e. $p = a^4 + b^4 + c^4 + d^4 + 3a^2b^2 + 11a^2c^2 + 18a^2d^2 + 3b^2c^2 + 11b^2d^2 + 3c^2d^2 - 6a^3c - 6ac^3 - 6b^3d - 6bd^3 - 14a^2bd - 4ab^2c - 14acd^2 - 4bc^2d + 12abcd$. Hence $p = u^2 + v^2 = z^2 + 5w^2$ with $u = a^2 + b^2 + c^2 + d^2 - 3ac - 3bd$, $v = 4ad - ab - bc - cd$, $z = a^2 - b^2 + c^2 - d^2 - 3ac + 3bd$ and $w = -2ad + ab - bc + cd$. The statement can now be shown as above, but also

[2] But note that the relevant form erroneously appears to be $x^2 + 16y^2$. In fact, Hasse proves a different criterion for primes $p \equiv 1 \pmod 8$ and refers to a private communication from Barrucand in which this was shown to be equivalent to $p = x^2 + 64y^2$. Hasse seems to have been unaware of Glaisher's results and also refers to much later works of Rédei and Reichardt regarding the criterion for $4 \mid h'$.

by brute force simply by letting $a, b, c, d$ run through all residue classes modulo 20 and checking the assertion in each case.

## References


[1] A. Aigner, *Kriterien zum 8. und 16. Potenzcharakter der Reste 2 und –2*, Deutsch. Math. **4** (1939), 44–52.

[2] P. Barrucand, H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70.

[3] D. Brink, *Five peculiar theorems on simultaneous representation of primes by quadratic forms*, J. Number Theory **129** (2009), 464–468.

[4] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, New York, 1989.

[5] J. W. L. Glaisher, *On the expressions for the number of classes of a negative determinant, and on the numbers of positives in the octants of $P$*, Quart. J. Pure Appl. Math. **34** (1903), 178–204.

[6] H. Hasse, *Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1$* mod. $2^3$, Aequationes Math. **3** (1969), 165–169.

[7] H. Hasse, *Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$*, J. Number Theory **1** (1969), 231–234.

[8] I. Kaplansky, *The forms $x + 32y^2$ and $x + 64y^2$*, Proc. Amer. Math. Soc. **131** (2003), no. 7, 2299–2300 (electronic).