MTH 411: Midterm exam 2 correction
Fall 2016

Exercise 1:

1) Show that the intersection of the subgroups $\langle 3\rangle$ and $\langle 15\rangle$ of U_{28} is $\{1\}$.

The successive powers of 3 modulo 28 are: 1,3,9,27 $= -1 \bmod 28$, $-3 = 25 \bmod 28$ and $-9 = 19 \bmod 28$, and we have $3^6 = 1 \bmod 28$.
On the other hand, $15^2 = 225 = 1 \bmod 28$. So $\langle 3\rangle = \{1, 3, 9, 27, 25, 19\}$ and $\langle 15\rangle = \{1, 15\}$ have trivial intersection.

2) Deduce from this that $U_{28} \simeq \mathbb{Z}_6 \times \mathbb{Z}_2$.

The group U_{28} as a set is $\{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$, so it has order 12. On the other $\langle 3\rangle \simeq \mathbb{Z}_6$ as 3 has order 6 and $\langle 15\rangle \simeq \mathbb{Z}_2$. These are normal subgroups (U_{28} is abelian) with trivial intersection, so the direct sum $\langle 3\rangle \oplus \langle 15\rangle$ is a subgroup of U_{28} isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$. Because it has order 12, this subgroup is actually U_{28}.

Exercise 2:

Let G be a group of order 380. We assume, by contradiction, that G is simple.
1) Compute the number of 5 and 19 Sylow subgroups of G.

By the third Sylow theorem, the number n_5 of 5-Sylow divides 76 and is 1 mod 5. Divisors of 76 are: 1,2,4,19,38 and 76. So $n_5 = 1$ or 76. As we assume G to be simple, $n_5 = 76$.
Similarly the third Sylow theorem gives you that $n_{19} = 1$ or 20, thus $n_{19} = 20$ if G is simple.

2) Show that G must contain at least 304 elements of order 5 and at least 360 elements of order 19. Conclude.

There are 76 5-Sylow subgroups, each of cardinal 5, thus isomorphic to $\mathbb{Z}_5$, thus containing 4 elements of order 5 and the identity element. The intersection of two of them must have cardinal a strict divisor of 5, thus it is only the identity elements. So we get $76 \times 4 = 304$ distincts elements of order 5.
Similarly, there are 20 19-Sylow subgroups, isomorphic to $\mathbb{Z}_{19}$, and their pairwise intersections are trivial, so we get 18×20 distincts elements of order 19.
As $304 + 360 > 380$, this is a contradiction, and a group of order 380 cannot be simple.

Exercise 3:

From Exam 1, you remember that the set $G = \{(a,b) \in \mathbb{R}^* \times \mathbb{R}\}$ is a group for the operation

$$(a,b)(c,d) = (ac, ad+b)$$

and that $N = \{(1,x) \text{ for } x \in \mathbb{R}^*\}$ is a normal subgroup of G.

1)Find the center Z of G.

(a,b) is in Z if for any $(c,d) \in G$, $(ac, ad+b) = (ca, cb+d)$. Taking $(c,d) = (1,2)$ you get $2a + b = b + 2$, thus $a = 1$. Taking $(c,d) = (2,0)$ you get $b = 2b$, thus $b = 0$. So the center is reduced to the identity element $(1,0)$.

2) Using the map φ :

$$\begin{aligned} G &\to \mathbb{R}^* \\ (a,b) &\mapsto a \end{aligned}$$

show that $G/N \simeq (\mathbb{R}^*, \times)$

The map φ is an homomorphism as

$$\varphi((a,b)(c,d)) = \varphi((ac, ad+b)) = ac = \varphi((a,b))\varphi((c,d))$$

The kernel of this map is $\{(a,b) \in G \ \ |a = 1\} = N$. The map is surjective as $\varphi((a,0)) = a$ for any $a \in \mathbb{R}^*$. The first isomorphism theorem says that $G/N \simeq \mathrm{Im}\varphi = \mathbb{R}^*$.

Exercise 4:

In $\mathbb{Z}[i]$, what is the gcd of $3 - 3i$ and $1 + 5i$?

Using Euclid's algorithm:

$$1 + 5i = \left(\frac{1+5i}{3-3i}\right)(3-3i) = \left(\frac{(1+5i)(3+3i)}{18}\right)(3-3i) = \left(\frac{-12+18i}{18}\right)(3-3i)$$

Approximating $\dfrac{-12+18i}{18}$ by the closest Gaussian integer $-1+i$, a Euclidian quotient is $-1+i$ and the remainder is then:

$$(1+5i) - (-1+i)(3-3i) = 1 - i$$

Now $1 - i$ divides $3 - 3i$, so their gcd is $1 - i$.
So $gcd(1+5i, 3-3i) = 1 - i$, up to a unit.