PRELIMINARY READING FOR ALGEBRAIC NUMBER THEORY. HT 2019.

Section 0. Background Material in Algebra and Number Theory

The following gives a summary of the main ideas you need to know as prerequisites to the Part B lecture course on Algebraic Number Theory. There is an associated optional Sheet 0 of questions for you to try, if you feel you need to refresh your skills in these topics. Most of you should have seen most of this material before in lecture courses from previous terms, but it is just as well to read through it carefully, in order to fill in any gaps.

Groups

Definition 0.1. A *group* is a set G with a binary operation $*$ which satisfies the following properties.
Closure: If $f, g \in G$ then $f * g \in G$.
Associativity: For all $f, g, h \in G$, $(f * g) * h = f * (g * h)$.
Existence of identity: There exists $e \in G$ such that, for all $g \in G$, $e * g = g * e = g$.
Existence of inverses: For all $g \in G$, there exists $h \in G$ such that $g * h = h * g = e$.

Comment 0.2. The element h is the *inverse* of g, and is typically denoted g^{-1}, when referring to a general group $G, *$, and any specific group whose operation is some type of multiplication. On the other hand, the inverse of g will typically be denoted $-g$ when dealing with a specific group whose operation is some form of addition.

Definition 0.3. We say that a group G is a *commutative* (or *Abelian*) group if it also satisfies *Commutativity:* For all $f, g \in G$, $f * g = g * f$.

Examples 0.4.
(a) $\mathbb{Z}, +$ is an Abelian group (identity 0).
(b) $\mathbb{Z}, \times$ has identity $= 1$ but, for example, 2 has no inverse, and so this is not a group.
(c) $\mathbb{R}^+, \times$ (the positive real numbers under multiplication) is an Abelian group with identity 1.
(d) $\mathbb{R} \times \mathbb{R}, +$ [which means all pairs (a, b), with operation $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$] is an Abelian group with identity $(0, 0)$.
(e) $\{2 \times 2$ matrices with nonzero determinant$\}$ under matrix multiplication is a group. Identity $= \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

(f) $C_6, +$ [the cyclic group of order 6], denoting $\{0, 1, 2, 3, 4, 5\}$ under $+$ modulo 6 [e.g. $3 + 4 = 1$]. This is an Abelian group with identity 0.
(g) $C_2 \times C_3, +$, which is $\{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$ under the operation: $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2 \bmod 2, b_1 + b_2 \bmod 3)$. This is an Abelian group with identity $(0, 0)$.
(h) Let $S_3, \circ$ be the set of permutations of $\{1, 2, 3\}$, with: $f \circ g =$ 'g-followed-by-f' as our operation [we shall normally abbreviate $f \circ g$ as fg]. This is a group and the elements are: $\{e, (12), (13), (23), (123), (132)\}$ [where, for example, (132) represents the permutation: $1 \to 3, 3 \to 2, 2 \to 1$, and (23) represents $2 \to 3, 3 \to 2$ (with $1 \to 1$)]. This is not an Abelian group since, for example, $(132)(12) = (23)$, but $(12)(132) = (13)$.

Definition 0.5. Let $G_1, *_1$ and $G_2, *_2$ be groups, and let $\phi : G_1 \to G_2$ [a map from G_1 to G_2]. We say that ϕ is a *homomorphism* if, for all $g, h \in G$, $\phi(g *_1 h) = \phi(g) *_2 \phi(h)$.

An *endomorphism* on a group G is a homomorphism from G to itself.

Examples 0.6.
(a) $\log : \mathbb{R}^+, \times \to \mathbb{R}, +$ is a homomorphism since, for all $a, b \in \mathbb{R}^+$, $\log(a \times b) = \log(a) + \log(b)$ [that is, $\log(a *_1 b) = \log(a) *_2 \log(b)$].
(b) $\phi : \mathbb{R} \times \mathbb{R}, + \to \mathbb{R}, +$ defined by $\phi\big((a, b)\big) = a$ [can also express this as $\phi : (a, b) \mapsto a$] is a homomorphism.
Proof. $\phi\big((a, b) *_1 (c, d)\big) = \phi\big((a, b) + (c, d)\big) = \phi\big((a + c, b + d)\big) = a + c$.

Also, $\phi\big((a, b)\big) *_2 \phi\big((c, d)\big) = \phi\big((a, b)\big) + \phi\big((c, d)\big) = a + c$, and these are the same.
(c) $\phi : \mathbb{Z}, + \to \mathbb{Z}, +$, defined by $\phi(a) = 2a$ is a homomorphism.
(d) $\phi : \mathbb{Z}, + \to \mathbb{Z}, + : a \mapsto a^2$ is not a homomorphism since, for example, $\phi(2 + 3) = \phi(5) = 5^2 = 25$, but $\phi(2) + \phi(3) = 2^2 + 3^2 = 13$, and these are not equal.

Definition 0.7. Let $\phi : S \to T$, for any sets S, T. We say that ϕ is *injective* (or 1–1 or an *injection*) if, for all $f, g \in S$, $\phi(f) = \phi(g) \implies f = g$; that is, $f \neq g \implies \phi(f) \neq \phi(g)$ [i.e. when it never happens that two distinct f and g are mapped by ϕ to the same element]. We say that ϕ is *surjective* (or *onto* or a *surjection*) if, for all $w \in T$, there exists $g \in S$ such that $w = \phi(g)$ [i.e. when every member of T is mapped onto by at least one element of S]. We say that ϕ is *bijective* (or a *bijection*) if it is both injective and surjective.

Definition 0.8. Let $\phi : G_1, *_1 \to G_2, *_2$ be a homomorphism. The *kernel* of ϕ (denoted $\ker \phi$) is defined as the set of all members of G_1 which are mapped to the identity element e_2 in G_2. That is: $\ker \phi = \{g \in G_1 : \phi(g) = e_2\}$. The image of ϕ (denoted $\operatorname{im} \phi$) is the set of all members of G_2 which are mapped onto by some member of G_1. That is to say: $\operatorname{im} \phi = \{\phi(g) : g \in G_1\}$.

Comment 0.9. Clearly, a homomorphism $\phi : G_1, *_1 \to G_2, *_2$ is injective if and only if $\ker \phi = \{e_1\}$, where e_1 is the identity element in G_1. It is surjective if and only if $\text{im } \phi = G_2$.

Examples 0.10.
(a) $\log : \mathbb{R}^+, \times \to \mathbb{R}, +$ is an injection since, for any $f, g \in \mathbb{R}^+$: $\phi(f) = \phi(g) \implies \log f = \log g \implies e^{\log f} = e^{\log g} \implies f = g$.

It is also a surjection since, if $w \in \mathbb{R}$, we can take $g = e^w \in \mathbb{R}^+$ and $\phi(g) = \log(e^w) = w$. Hence ϕ is a bijection, since it is both an injection and a surjection. The kernel is $\{1\}$ [that is, 1 is the unique member of $\mathbb{R}^+, \times$ mapped by log to the identity element 0 in $\mathbb{R}, +$]. The image is all of $\mathbb{R}$ [since the map is surjective].
(b) Let $\phi : \mathbb{R} \times \mathbb{R}, + \to \mathbb{R}, +$ be defined by $\phi\big((a, b)\big) = a$. This is not an injection since, for example, $\phi\big((2, 1)\big) = 2$ and $\phi\big((2, 3)\big) = 2$, but $(2, 1) \neq (2, 3)$. It is a surjection since, for any $r \in \mathbb{R}$, we can take $(r, 0) \in \mathbb{R} \times \mathbb{R}$ which satisfies $\phi\big((r, 0)\big) = r$ [of course, we could just as easily have used $(r, 1)$; we merely had to show that every $r \in \mathbb{R}$ is mapped onto by at least one member of of $\mathbb{R} \times \mathbb{R}$]. The kernel is $\{(0, b) : b \in \mathbb{R}\}$ and the image is all of $\mathbb{R}$ [since ϕ is surjective].
(c) $\phi : \mathbb{Z}, + \to \mathbb{Z}, +, a \mapsto 2a$. This is an injection since, for any $a, b \in \mathbb{Z}$: $\phi(a) = \phi(b) \implies 2a = 2b \implies a = b$. It is not a surjection since nothing maps to 3 (for example). The kernel is $\{0\}$ and the image is $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$.

Definition 0.11. Let $G_1, *_1$ and $G_2, *_2$ be groups and let $\phi : G_1 \to G_2$. If ϕ is both a bijection and a homomorphism, then we say that ϕ is an *isomorphism*. If there exists an isomorphism $\phi : G_1 \to G_2$, we say that the two groups are *isomorphic* (same shape) and we write $G_1 \cong G_2$.

Comment 0.12. If G_1 and G_2 are isomorphic groups, then G_2 can be regarded as the same group as G_1, merely with the elements relabelled. G_1 and G_2 will have all of the same structural properties (for example, G_1 will be Abelian iff G_2 is Abelian, G_1 will have an element $g \neq e$ satisfying $g * g = e$ iff G_2 has such an element, etc).

Example 0.13. $\log : \mathbb{R}^+, \times \to \mathbb{R}, +$ is an isomorphism, since it is both a homomorphism and a bijection. The groups $\mathbb{R}^+, \times$ and $\mathbb{R}, +$ are isomorphic.

Comment 0.14. Two finite groups G_1, G_2 are isomorphic if the group table of G_1 can have its elements relabelled to give the group table of G_2.

Example 0.15. Let $G_1 = C_2 \times C_3$ and $G_2 = C_6$. Let $\phi : G_1 \to G_2$ be defined by:
$(0, 0) \mapsto 0,\ (1, 1) \mapsto 1,\ (0, 2) \mapsto 2,\ (1, 0) \mapsto 3,\ (0, 1) \mapsto 4,\ (1, 2) \mapsto 5.$
The group table of G_1 is as follows.

+	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,1)	(1,1)	(0,2)	(0,0)	(0,1)

Replacing all entries using ϕ gives the following table.

+	0	4	2	3	1	5
0	0	4	2	3	1	5
4	4	2	0	1	5	3
2	2	0	4	5	3	1
3	3	1	5	0	4	2
1	1	5	3	4	2	0
5	5	3	1	2	0	4

This is just the group table for C_6, which proves that $C_2 \times C_3 \cong C_6$.

The last example is a special case of the following result.

Lemma 0.16. *When $m, n \in \mathbb{Z}$ and m, n have no common factors (apart from 1) then $C_m \times C_n \cong C_{mn}$.*

The following is also quite a useful property of finite Abelian groups.

Lemma 0.17. *Any finite Abelian group G is isomorphic to the product of cyclic groups: $G \cong C_{m_1} \times C_{m_2} \times \ldots \times C_{m_k}$, for some $C_{m_1}, \ldots, C_{m_k}$.*

For any group G, it is natural to consider groups which lie inside G (that is to say, which are subsets of G).

Definition 0.18. Let $G, *$ be a group and let $H \subset G$ [H is a subset of G]. We say that H is a *subgroup* of G (written: $H \leqslant G$) if H is nonempty, and forms a groups with respect to the same operation $*$ as G. This is equivalent to:

$e_G \in H$ (where e_G is the identity element in G),

If $f, g \in H$ then $f * g \in H$,

If $h \in H$ then $h^{-1} \in H$. Note that associativity automatically holds in H since it holds in the group G, of which H is a subset.

Examples 0.19.

(a) $H = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \leqslant \mathbb{Z}, +$.

(b) $H = \{\ldots, -3, -1, 1, 3, \ldots\} \not\leqslant \mathbb{Z}, +$, since the identity element 0 is not in the set (we could alternatively have used the fact that it is not closed; for example, $1, 3 \in H$ but $1 + 3 \notin H$).

(c) $H = \{0, 1, 2, 3, \ldots\} \not\leqslant \mathbb{Z}, +$. It is fine for containing the identity element and closure, but H does not contain the inverse of every element in H (for example, $3 \in H$ but $-3 \notin H$).

Definition 0.20. Let $H \leqslant G$ and let $g \in G$. The set $gH = \{g * h : h \in H\}$ is called a *left coset* of H and the set $Hg = \{h * g : h \in H\}$ is called a *right coset* of H. When the number of distinct left cosets is finite, it can be shown that this is the same as the number of distinct right cosets; this number is the *index* of H in G and is denoted $[G : H]$.

Comment 0.21. When the group operation is some form of multiplication, one typically writes the left (or right) cosets, as above, in the style gH (or Hg). When the group operation is some form of addition, then one typically writes $g + H = \{g + h : h \in H\}$ (similarly for $H + g$).

Example 0.22. Let $G = \mathbb{Z}, +$ and let $H = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \leqslant G$. Then some examples of left cosets are:

$0 + H = \{\ldots, 0 + (-6), 0 + (-3), 0 + 0, 0 + 3, 0 + 6, \ldots\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$,
$1 + H = \{\ldots, 1 + (-6), 1 + (-3), 1 + 0, 1 + 3, 1 + 6, \ldots\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$,
$2 + H = \{\ldots, 2 + (-6), 2 + (-3), 2 + 0, 2 + 3, 2 + 6, \ldots\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$,
$3 + H = \{\ldots, 3 + (-6), 3 + (-3), 3 + 0, 3 + 3, 3 + 6, \ldots\} = \{\ldots, -3, 0, 3, 6, 9, \ldots\}$.
$4 + H = \{\ldots, 4 + (-6), 4 + (-3), 4 + 0, 4 + 3, 4 + 6, \ldots\} = \{\ldots, -2, 1, 4, 7, 10, \ldots\}$.

Note that $0 + H = 3 + H$ and $1 + H = 4 + H$. Clearly

$\ldots -6 + H = -3 + H = 0 + H = 3 + H = 6 + H = \ldots$
$\ldots -5 + H = -2 + H = 1 + H = 4 + H = 7 + H = \ldots$
$\ldots -4 + H = -1 + H = 2 + H = 5 + H = 8 + H = \ldots$

so that there are only 3 distinct left cosets. So here the index $[G : H] = 3$.

The left coset $eH = H$, where e is the identity element, so that H is one of the left cosets of itself (and similarly is one of the right cosets of itself). It can be shown that two left cosets g_1H and g_2H are either equal or disjoint and that every element of G is a member of some coset. When G is a finite group, it can also be shown that any g_1H and g_2H have the same number of elements (and so every left coset of H has the same number of elements as H). It follows that the left cosets of H give a partition of G, that is, they give G as a union of disjoint subsets. Since each of these subsets has the same number of elements as H, we see that $|G| = |H| + \ldots + |H| = k|H|$, where k is the number of distinct left cosets of H [here, $|S|$ is the standard notation for the number of elements in S, for any set S]. The following immediately follows.

Theorem 0.23. *(Lagrange's Theorem) Let G be a finite group, and let $H \leqslant G$. Then $|H|$ is a factor of $|G|$ [this can also be expressed as $|H|$ divides $|G|$, or as $|H| \mid |G|$].*

There are many situations where we would like to consider the elements of a group G, but in a simplified context, where we 'mod out' (or 'quotient out') by a subgroup, and focus on the information that remains. For example, when $G = \mathbb{Z}, +$, we might want to collapse $H = 3\mathbb{Z} \leqslant G$ down to a single element, and consider the elements mod H (considering elements to be the same if they lie in the same coset). The natural way to do this is to create a new group G/H, whose elements are (say) the left cosets of H, in which case there are only 3 distinct elements:

$$\{\ldots, -6, -3, 0, 3, 6, \ldots\}, \{\ldots, -5, -2, 1, 4, 7, \ldots\}, \{\ldots, -4, -1, 2, 5, 8, \ldots\},$$

which give all the members of G/H. It is natural to ask whether the group law on G carries over to give group law on G/H. How might we add, for example, the second and third of these? That is, we want to perform the addition:

$$\{\ldots, -5, -2, 1, 4, 7, \ldots\} + \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

A natural attempt is add any element in the first coset to any element in the second coset, and see what coset the sum lies in. For example, -5 is in the first coset, and 2 is the second coset, and $-5 + 2 = -3$, which lies in: $\{\ldots, -6, -3, 0, 3, 6, \ldots\}$, suggesting that, in G/H:

$$\{\ldots, -5, -2, 1, 4, 7, \ldots\} + \{\ldots, -4, -1, 2, 5, 8, \ldots\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}.$$

Furthermore, it doesn't matter what members you take: you can add any member of $\{\ldots, -5, -2, 1, 4, 7, \ldots\}$ to any member of $\{\ldots, -4, -1, 2, 5, 8, \ldots\}$ and you will get a member of $\{\ldots, -6, -3, 0, 3, 6, \ldots\}$, reinforcing our confidence in this definition of the sum. It is easy to see that this gives a way of turning the 3 members of G/H into a group. We can also express this group law on G/H as: $(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H$, where the well-definedness of this rule is due to the fact that, at least for this choice of G, H, whenever $g_1 + H = g_1' + H$ and $g_2 + H = g_2' + H$ then $(g_1 + g_2) + H = (g_1' + g_2') + H$. Even though the members of G/H are sets, it is often convenient to denote them by selected representative elements; for example, we can use $0, 1, 2$ to denote the cosets containing $0, 1, 2$, respectively, in which case that above addition could be expressed as: $1 + 2 = 0$ in G/H. Of course, 91 lies in the same coset as 1, so that $1 = 91$ in G/H; we could just as easily represent our 3 members of G/H as $0, 91, 2$ and say that $91 + 2 = 0$ in G/H.

Similarly, let $G = \mathbb{C}^*, \times$, the group of nonzero complex numbers under multiplication, and let $H = \{z : |z| = 1\} \leqslant G$, the unit circle on an Argand diagram. Then an example of a left coset is $(3 + 4i)H = \{(3 + 4i)z : |z| = 1\}$, which is easily seen to be just the circle, centre 0, with radius 5 (the modulus of $3 + 4i$). Note that the group operation is multiplication here, so the cosets are written as $gH = \{g * h : h \in H\} = \{gh : h \in H\}$ [rather than $g + H = \{g * h : h \in H\} = \{g + h : h \in H\}$, as in the previous example]. Two complex

numbers are in the same coset iff they have the same modulus. Clearly, the left cosets are just the circles with centre 0, and these are the elements of G/H. We have 'modded out' by H, removing the argument information, and retaining only the modulus information. We can turn G/H into a group under multiplication: for example, the set of complex numbers of modulus 5 multiplied by the set of complex numbers of modulus 2 gives the set of complex numbers modulus 10. This is well defined, since it does not matter which representative is taken: any member of the first coset (any complex number of modulus 5) times any member of the second coset (any complex number of modulus 2) will give a member of the third coset (a complex number of modulus 10).

By way of contrast, let G be as in Example **??**(h), that is, $G = S_3, \circ$, the group of permutations of $\{1, 2, 3\}$ under the operation $f \circ g =$ 'g-followed-by-f' [where, as usual, we shall abbreviate $f \circ g$ as fg]. Consider $H = \{e, (12)\} \leqslant G$. There are only 3 distinct left cosets of H:

$eH = (12)H = \{e, (12)\}$,
$(123)H = (13)H = \{(123), (13)\}$,
$(132)H = (23)H = \{(132), (23)\}$.

How might we try to perform: $\{e, (12)\}\{(123), (13)\}$? We could attempt the same approach as before: take any element from each set, combine them according to the group law on G and see what coset the results lies in. For example, e is a member of $\{e, (12)\}$ and (123) is a member of $\{(123), (13)\}$ and $e(123) = (123) \in \{(123), (13)\}$. So we might be tempted to say that $\{e, (12)\}\{(123), (13)\} = \{(123), (13)\}$. On the other hand, $(12) \in \{e, (12)\}$ and $(13) \in \{(123), (13)\}$, and $(12)(13) = (132) \in \{(132), (23)\}$, so this suggests that $\{e, (12)\}\{(123), (13)\} = \{(132), (23)\}$. We see that there is no sensible unambiguous way of defining $\{e, (12)\}\{(123), (13)\}$. To put it another way, our attempt to use the natural rule $(g_1H)(g_2H) = (g_1g_2)H$ to give a group law on G/H, has foundered on the fact that there are instances where $g_1H = g_1'H$ and $g_2H = g_2'H$, but $(g_1g_2)H \neq (g_1'g_2')H$ [for example, when $g_1 = e, g_1' = (12), g_2 = (123), g_2' = (13)$]. Any attempt to turn the set of right cosets into a group would also suffer the same problem. Note that if we keep the group $G = S_3$, as before, but use instead $H = \{e, (123), (132)\} \leqslant G$, then it is easy to check that everything is fine, and we can turn G/H into a group.

The key property which allows G/H to be a group is the following.

Definition 0.24. Let $G, *$ be a group and let $H \leqslant G$. We say that H is a *normal* subgroup of G, denoted $H \lhd G$ if, for every $g \in G$, $gH = Hg$.

An equivalent definition is: $\forall g \in G,\ \forall h \in H,\ \ g^{-1}hg \in H$.

Comment 0.25. When $H \lhd G$, the left cosets of H are the same as the right cosets, and so we can just refer to them as *cosets*, without needing to specify left or right.

Definition 0.26. Let $G, *$ be a group and let $H \lhd G$. Then G/H (or 'G quotient H' or 'G mod H') is defined as $G/H = \{gH : g \in G\}$, under the group operation: $(g_1H)(g_2H) = (g_1g_2)H$ [here, we are writing g_1g_2, g_1H, g_2H as shorthand for $g_1 * g_2, g_1 * H, g_2 * H$].

When G/H is finite then clearly $\#G/H = [G : H]$ (since the elements of G/H are the distinct cosets of H in G, and the number of these is defined to be the index $[G : H]$).

Why is it that the condition $H \lhd G$ is sufficient for this group operation on G/H to be well defined? Recall, the guarantee we need for unambiguity is that, whenever $g_1H = g_1'H$ and $g_2H = g_2'H$, then $(g_1g_2)H = (g_1'g_2')H$. So, suppose that $H \lhd G$ and that $g_1H = g_1'H, g_2H = g_2'H$. Then:

$$\begin{aligned}(g_1g_2)H &= g_1(g_2H) = g_1(g_2'H) = g_1(Hg_2') = (g_1H)g_2' \\ &= (g_1'H)g_2' = (Hg_1')g_2' = H(g_1'g_2') = (g_1'g_2')H, \text{ as required.}\end{aligned}$$

Comment 0.27. If $G, *$ is Abelian then any subgroup H must be normal, guaranteeing that we can always form the quotient group G/H.

Definition 0.28. Let X be any set, and let $\sim$ be a binary relation on X. We say that $\sim$ is an *equivalence relation* if it satisfies:

(1) $a \sim a$ for all $a \in X$ [reflexivity].

(2) $a \sim b \implies b \sim a$ for all $a, b \in X$ [symmetry].

(3) $a \sim b$ and $b \sim c \implies a \sim c$ for all $a, b, c \in X$ [transitivity].

The *equivalence class* of an element $a \in X$, denoted $[a]$, is the set of all members of X which are equivalent to a. This is to say: $[a] = \{x \in X : x \sim a\}$.

Given any $g_1, g_2 \in G$, it is easy to check that $g_1H = g_2H$ exactly when $g_1 = g_2 * h$, for some $h \in H$; that is, when $g_1 * g_2^{-1} \in H$. Define the relation $g_1 \sim g_2$ by:

$$g_1 \sim g_2 \iff g_1 = g_2 * h, \text{ for some } h \in H,$$

which gives an equivalence relation on G. Another way to describe members of G/H is to say that they are equivalence classes under this relation (or, we can also say that they are the members of G *modulo* the equivalence relation).

Comment 0.29. It can sometimes seem cumbersome to deal directly with the above definition of G/H, since the group elements in G/H are cosets (so that G/H is a set of sets). Suppose nobody had ever mentioned cosets. There is a more intuitive approach to quotient groups (which is in fact the way they are mostly dealt with in practice) which requires no

explicit mention of cosets. Namely, one writes the elements of G/H exactly as the elements of G, except that certain elements become equal in G/H which were distinct in G. Specifically, one imposes the rule:

$$g_1 = g_2 \text{ in } G/H \iff g_1 = g_2 * (\text{some member of } H).$$

Equivalently: $g_1 = g_2$ in $G/H \iff g_1 * g_2^{-1} \in H$. When the operation in G is addition, this means two elements are equal in G/H exactly when their difference is in H. When the operation in G is multiplication, two elements are equal in G/H exactly when their quotient is in H [of course, when the group operation is neither an addition nor a multiplication, then just use the general criterion $g_1 * g_2^{-1} \in H$]. The following examples are described in this spirit, with no explicit mention of cosets.

Examples 0.30.

(a) Let $G = \mathbb{Z}, +$ and $H = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \leqslant G$. We see that, for example, $1 = 16 * (-15)$ in G [since $*$ is $+$ here], so that $1 = 16 * (\text{member of } H)$, and so $1 = 16$ in G/H. Equivalently, $1 * 16^{-1} = 1 + (-16) = -15 \in H \implies 1 = 16$ in G/H [note that 16^{-1} is the inverse of 16 in G, which is -16]. On the other hand, $1 \neq 20$ in G/H, since $1 = 20 * (-19)$ and $-19 \notin H$.

In the group $G/H = \mathbb{Z}/3\mathbb{Z}$:

$\ldots = -6 = -3 = 0 = 3 = 6 = \ldots$

$\ldots = -5 = -2 = 1 = 4 = 7 = \ldots$

$\ldots = -4 = -1 = 2 = 5 = 8 = \ldots$

and so $\mathbb{Z}/3\mathbb{Z}$ contains only 3 distinct elements. The usual convention is to pick out $0, 1, 2$ as listing the distinct members of $\mathbb{Z}/3\mathbb{Z}$. We can see that $\mathbb{Z}/3\mathbb{Z}, +$ is isomorphic to $C_3, +$.

(b) Let $G = \mathbb{Q}^*, \times$ = nonzero members of $\mathbb{Q}$ under multiplication. Let $H = (\mathbb{Q}^*)^2 = \{\text{squares of nonzero members of } \mathbb{Q}\}$. For example, $4/9 \in H$ but $2 \notin H$.

In $\mathbb{Q}^*$, $2/3 = 6 \times \frac{1}{9}$ and $\frac{1}{9} \in (\mathbb{Q}^*)^2$ so that $2/3 = 6$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Similarly, $6 = \frac{24}{25}$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ since $6 = \frac{24}{25} \times \frac{25}{4}$ and $\frac{25}{4} \in (\mathbb{Q}^*)^2$. However, $2 \neq 3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ since $2 = 3 \times \frac{2}{3}$ and $\frac{2}{3} \notin (\mathbb{Q}^*)^2$.

Note that any $\frac{a}{b} \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ [where $a, b \in \mathbb{Z}$] can be written as $\frac{a}{b} = \frac{a}{b}b^2 = ab \in \mathbb{Z}$. We can write any integer in the form rs^2 where $r, s \in \mathbb{Z}$ and r is square-free [where *square free* means not divisible by any integer square except 1; for example, 6 is square free, but 12 is not square free, since it is divisible by 4]. Write the integer ab in the form rs^2, so that $\frac{a}{b} = ab = rs^2 = r$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. The standard way of working in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is to write each distinct element as a square free integer. For example:

$\frac{20}{13} = \left(\frac{20}{13}\right)13^2 = 20 \times 13 = 4 \times 5 \times 13 = 5 \times 13 = 65$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$,

which is a square free integer.

(c) Let $G = \mathbb{C}^*, \times$ and $H = \{z : |z| = 1\}$. Then $z_1 = z_2$ in $G/H \iff z_1/z_2 \in H \iff |z_1/z_2| = 1 \iff |z_1| = |z_2|$. That is, $z_1 = z_2$ in G/H exactly when they have the same modulus. So, for example, $3 + 4i = 5i = 5$ in G/H. Clearly, every member of G is equal in G/H to precisely one nonzero real number (namely, its modulus). So, each element of G/H can be represented by a nonzero real numbers, and it is easy to see that G/H is isomorphic to $\mathbb{R}^*, \times$.

Given a homomorphism $\phi : G_1, *_1 \to G_2, *_2$, the kernel can be shown to be a normal subgroup of G_1, and so we can form the quotient group $G_1/\ker\,\phi$. The map $g *_1 \ker\,\phi \mapsto g$ can be shown to be well defined and injective (and onto im ϕ), giving the following result.

Theorem 0.31. *[First Isomorphism Theorem for Groups] Let $\phi : G_1, *_1 \to G_2, *_2$ be a homomorphism. Then $\ker\,\phi \lhd G_1$, $\text{im}\,\phi \leqslant G_2$ and $G_1/\ker\,\phi \cong \text{im}\,\phi$. In particular, if ϕ is surjective then $G_1/\ker\,\phi \cong G_2$.*

Comment 0.32. Note that, in the case when ϕ is surjective, we have im $\phi = G_2$ and so $G_1/\ker\,\phi \cong G_2$.

Examples 0.33.
(a) Let $\phi : \mathbb{R} \times \mathbb{R} \times \mathbb{R}, + \to \mathbb{R} \times \mathbb{R}, +$ be defined by $\phi\big((x, y, z)\big) = (x, y)$ [the projection map to the (x, y)-plane]. Then $\ker\,\phi$ is the z-axis $\{(0, 0, z) : z \in \mathbb{R}\}$, and im ϕ is all of $\mathbb{R} \times \mathbb{R}$ (the map is surjective). The isomorphism theorem tells us that $\mathbb{R} \times \mathbb{R} \times \mathbb{R}/\ker\,\phi \cong \mathbb{R} \times \mathbb{R}$.
(b) Let $\phi : \mathbb{C}^*, \times \to \mathbb{R}^*, \times : z \mapsto |z|$. Then $\ker\,\phi = \{z : |z| = 1\}$ and im ϕ is all of $\mathbb{R}$ (the map is surjective). The isomorphism theorem tells us that $\mathbb{C}^*/\ker\,\phi \cong \mathbb{R}^*$.

The following are both easy to deduce from the First Isomorphism Theorem.

Theorem 0.34. *[Second Isomorphism Theorem for Groups] Let $H \leqslant G$ and $N \lhd G$. Then $HN \leqslant G$, $H \cap N \lhd H$ and $(HN)/N \cong H/(H \cap N)$.*

Theorem 0.35. *[Third Isomorphism Theorem for Groups] Let $N \lhd G, K \lhd G$, with $K \subseteq N \subseteq G$. Then $N/K \lhd G/K$ and $(G/K)/(N/K) \cong G/N$.*

The proof of the last part is simply to consider the natural map : $G/K \to G/N : g + K \mapsto g + N$, check that it is a well defined surjective homomorphism with kernel N/K and then apply the First Isomorphism Theorem.

Another important idea is that of the order of an element.

Definition 0.36. Let $G, *$ be a group and $g \in G$. If there exists $k > 0$ such that $g * g * \ldots * g$ [k times] $= e$ then we say that g has *finite order* (or is a *torsion* element), and the smallest such k is the *order* of g, denoted $\text{o}(g)$. If no such k exists, we say that g has *infinite order*.

For an Abelian group G, the set of all elements in G of finite order is a subgroup of G, the *torsion subgroup* of G, denoted G_{tors}.

Since $\{e, g, g^2, \ldots, g^{o(g)-1}\}$ is a subgroup of G [the *subgroup generated by* g] with $o(g)$ elements, we obtain the following consequence of Lagrange's Theorem.

Corollary 0.37. *Let $G, *$ be a group and $g \in G$. The order of g is always a factor of $|G|$. As a consequence, $g^{|G|} = e$.*

There is a partial converse due to Cauchy.

Theorem 0.38. *[Cauchy's Theorem on Finite Groups] Let G be a finite group and let p be prime such that p divides $|G|$. Then there exists $g \in G$ such that $o(g) = p$.*

Definition 0.39. We say that $G, *$ is *Boolean* if, for all $g \in G$, $g * g = e$ [and so every element apart from the identity will have order 2].

Comment 0.40. Any finite Boolean group G is isomorphic to the product of a finite number of copies of C_2; that is: $G \cong C_2 \times C_2 \times \ldots \times C_2$. It follows that the order of G [that is, the number of elements in G] is a power of 2.

Definition 0.41. Let $G, *$ be an Abelian group. The *m-torsion subgroup* of G, denote by $G[m]$, is defined as $\{g \in G : g * g * \ldots * g \ [m \text{ times}] \ = e\}$. This is same as the set of members of G whose orders are factors of m.

Comment 0.42. When G be an Abelian group, let $2G$ denote the subgroup $\{g * g : g \in G\}$. Clearly $G/2G$ is always a Boolean group When G is a finite Abelian group, it can be shown that $G/2G \cong G[2]$.

Definition 0.43. Let G be a group, written additively (so that our operation is written $+$). Let $H_1, \ldots, H_n \leqslant G$. We say that $G = \oplus_{i=1}^{n} H_i = H_1 \oplus \ldots \oplus H_n$ if every $g \in G$ can be written uniquely as $g = h_1 + \ldots + h_n$, where each $h_i \in H_i$.

Definition 0.44. Let G be a group, written additively, and let $g \in G$. For any positive $a \in \mathbb{Z}$, define $ag = g + \ldots + g$ [a times]; define $(-a)g = -(ag)$; also define $0g$ to be the group identity (so, we have now defined ag for any $a \in \mathbb{Z}$). We say that G is a *free abelian group* if there exists a set S of elements of G for which every $g \in G$ can be written uniquely as a linear combination of a finite number of elements of S, with integer coefficients (up to isomorphism, it is just the set of formal finite sums of members of S). We say that S is a $\mathbb{Z}$-basis for G. When S is finite and $|S| = n$, we say that G is a free abelian group *of rank* n.

For example $G = \mathbb{Z} \times \mathbb{Z}$ (under addition) is a free abelian group of rank 2, with $\mathbb{Z}$-basis $S = \{(1,0),(0,1)\}$, since any $(a,b) = G$ can be written uniquely as $a(1,0) + b(0,1)$, for $a, b \in \mathbb{Z}$.

Suppose G is any free abelian group of rank n with $\mathbb{Z}$-basis $S = \{w_1, \ldots, w_n\}$; then $G = \mathbb{Z}w_1 \oplus \ldots \oplus \mathbb{Z}w_n$; furthermore G and $\mathbb{Z} \times \cdots \times \mathbb{Z}$ (n times), are isomorphic as additive groups.

Elementary Number Theory

We have already seen the idea of the 'integers modulo m' developed as a quotient group in Example **??**(a). The next few definitions rephrase this idea in the language of congruences (which we have already used in Examples **??**(f),(g), but which we now formalise). First a few preliminaries are necessary.

Definition 0.45. For any $a, b \in \mathbb{Z}$, we say that a *divides* b [or that a is a *factor* of b, or that a is a *divisor* of b], denoted $a|b$, if there exists $k \in \mathbb{Z}$ such that $b = ka$. When a does not divide b, this is denoted $a \nmid b$ [for example, $5|20$, but $7 \nmid 20$ and $20 \nmid 5$].

Example 0.46. If $x \in \mathbb{Z}$ is a root of a polynomial $f(x) = f_n x^n + \ldots + f_0$ with integer coefficients, then $x|f_0$ [since, $f(x) = 0$ implies $x(-f_n x^{n-1} - \ldots - f_1) = f_0$]. So, for example, to test whether $x^3 + 11x - 6 = 0$ has any integer solutions, it is only necessary to check the possibilities $x = \pm 1, \pm 2, \pm 3, \pm 6$. Since none of these are solutions, it follows that the equation $x^3 + 11x - 6 = 0$ has no integer solutions.

Definition 0.47. Let $m \in \mathbb{Z}, m > 1$. We say that m is *prime* [or a *prime number*] if its only divisors are 1 and m itself; otherwise m is *composite* [by convention, 1 is neither prime nor composite].

Definition 0.48. For any $m, n \in \mathbb{Z}$, the *highest common factor* of m, n, denoted $\mathrm{hcf}(m,n)$, is the largest $d \geqslant 1$ such that $d|m$ and $d|n$ (sometime also called the *greatest common divisor* of m, n or $\gcd(m,n)$). The *least common multiple* of m, n, denoted $\mathrm{lcm}(m,n)$, is the smallest $D \geqslant 1$ such that $m|D$ and $n|D$. Sometimes $\mathrm{hcf}(m,n)$ is abbreviated as (a,b) and $\mathrm{lcm}(m,n)$ as $[a,b]$. When $\mathrm{hcf}(m,n) = 1$ we say that m and n are *coprime*.

For example, the positive divisors of 12 are: $1, 2, 3, 4, 6, 12$ and the positive divisors of 18 are: $1, 2, 3, 6, 9, 18$. The common divisors are: $1, 2, 3, 6$, the greatest of which is 6, and so $\mathrm{hcf}(12, 18) = 6$.

Note that any common divisor of a and b is also a common divisor of $a + kb$ and b, and vice versa, giving the following property of hcf's.

Lemma 0.49. *For any $a, b, k \in \mathbb{Z}$, $hcf(a + kb, b) = hcf(a, b) = hcf(a, b + ka)$.*

A fundamental property of $\mathbb{Z}$ is that, given any $a, b \in \mathbb{Z}$, one can find the highest multiple of b [say qb] $\leqslant a$, and the remainder $a - qb$ will have absolute value less than $|b|$. This is to say, given any $a, b \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $|r| < |b|$. This is known as the *Division Algorithm*, and the existence of such q, r [given any a, b] can be proved by induction. For example, given $a = 22$ and $b = 5$, we can say that 5 goes into 22 a total of $q = 4$ times with remainder $r = 2$, and write: $22 = 4 \cdot 5 + 2$, and indeed $0 \leqslant 2 < 5$. Repeated applications of the Division Algorithm give the following technique for finding the greatest common divisor of two numbers.

Definition 0.50. Given positive integers m, n, *Euclid's Algorithm* for finding $\text{hcf}(m, n)$ is as follows.

First find q_1, r_2 such that $m = q_1 n + r_2 \;\; (0 \leqslant r_2 < n)$,

Then find q_2, r_3 such that $n = q_2 r_2 + r_3 \;\; (0 \leqslant r_3 < r_2)$,

Then find q_3, r_4 such that $r_2 = q_3 r_3 + r_4 \;\; (0 \leqslant r_4 < r_3)$, and so on.

Since the remainders $r_i \geqslant 0$ are strictly decreasing, we will at some point get remainder 0. The last nonzero remainder r_k is $\text{hcf}(m, n)$.

The proof that Euclid's Algorithm gives $\text{hcf}(m, n)$ is a repeated application of Lemma **??**.

Example 0.51. Consider $m = 9108, n = 1121$. The first step of Euclid's Algorithm is: $9108 = 8{\cdot}1121{+}140$. The second step is: $1121 = 8{\cdot}140{+}1$, and the final step is $140 = 140{\cdot}1 = 0$, giving remainder 0. The last nonzero remainder is 1, which must be $\text{hcf}(9108, 1121)$.

Note that we can reverse the steps of Euclid's Algorithm to express $\text{hcf}(m, n)$ as an integer linear combination of m, n. In this example, we write the equation from the last-nonzero-remainder step as: $1 = 1121 - 8 \cdot 140$. We then use the previous equation [expressed as $140 = 9108 - 8{\cdot}1121$] to obtain: $1 = 1121 - 8{\cdot}(9108 - 8{\cdot}1121)$ and so $1 = -8{\cdot}9108 + 65{\cdot}1121$.

Another way of performing the same computation is by row operations on the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \middle| \begin{smallmatrix} m \\ n \end{smallmatrix}\right)$. In this case:

$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \middle| \begin{smallmatrix} 9108 \\ 1121 \end{smallmatrix}\right) \to^{R_1 - 8R_2} \left(\begin{smallmatrix} 1 & -8 \\ 0 & 1 \end{smallmatrix} \middle| \begin{smallmatrix} 140 \\ 1121 \end{smallmatrix}\right) \to^{R_2 - 8R_1} \left(\begin{smallmatrix} 1 & -8 \\ -8 & 65 \end{smallmatrix} \middle| \begin{smallmatrix} 140 \\ 1 \end{smallmatrix}\right) \to^{R_1 - 140R_2} \left(\begin{smallmatrix} * & * \\ -8 & 65 \end{smallmatrix} \middle| \begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$,

where the $*$ entries need not be computed. This gives us, all in the same computation, that $\text{hcf}(9108, 1121) = 1$, and the bottom row of the last matrix gives $\text{hcf}(9108, 1121)$ as a linear combination of $9108, 1121$, namely: $1 = -8 \cdot 9108 + 65 \cdot 1121$, as before.

This process can be performed for any m, n, giving the following result.

Lemma 0.52. *For any $m, n \in \mathbb{N}$, there exist $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = hcf(m, n)$.*

Definition 0.53. Let $a, b, m \in \mathbb{Z}$. We say that $a \equiv b \pmod{m}$ ['a is congruent to b modulo m'] when $m | (a - b)$.

For example, $2 \equiv 12 \pmod 5$, since $5|(2-12)$. It is straightforward to show that, if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

$a+c \equiv b+d,\ a-c \equiv b-d,\ ac \equiv bd,\ a^n \equiv b^n,\ ka \equiv kb \pmod n$,

for any $k \in \mathbb{Z}$ and any $n \in \mathbb{Z}, n \geqslant 0$. So, congruences in most ways can be manipulated like standard equations. An exception is cancellation: $ka \equiv kb \pmod m$ does not always imply that $a \equiv b \pmod m$; for example $2 \cdot 4 \equiv 2 \cdot 1 \pmod 6$ even though $4 \not\equiv 1 \pmod 6$. However, the implication is always true when k and m are coprime.

Lemma 0.54. *If hcf$(m,n) = 1$ then there exists $\lambda \in \mathbb{Z}$ such that $\lambda m \equiv 1 \pmod n$. In particular, if p is prime and $p \nmid m$ then there exists $\lambda \in \mathbb{Z}$ such that $\lambda m \equiv 1 \pmod p$.*

Proof We know from Lemma **??** that there exist λ, μ such that $\lambda m + \mu n = \text{hcf}(m,n)$. Reducing modulo n immediately gives the required result. □

Corollary 0.55. *For any $m \in \mathbb{N}$, the set $G_m = \{x : 1 \leqslant x \leqslant m, \text{hcf}(x,m) = 1\}$ is a group under multiplication modulo m. In particular, for any prime p, the set $\{1, 2, \ldots, p-1\}$ is a group under multiplication modulo p.*

Letting $G = \{1, 2, \ldots, p-1\}$, we can apply Corollary **??** to obtain the following.

Theorem 0.56. *(Fermat's Little Theorem). Let p be prime. If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$.*

As a consequence, $a^p \equiv a \pmod p$ for all a, regardless of whether $p|a$ or $p \nmid a$.

The following result is useful for solving simultaneous congruences.

Theorem 0.57. *[Chinese Remainder Theorem (for congruences)] Let $n_1, \ldots, n_k \in \mathbb{Z}$ be pairwise coprime (that is, hcf$(n_i, n_j) = 1$ whenever $i \neq j$). Let $a_1, \ldots, a_k \in \mathbb{Z}$. Then there exists $x \in \mathbb{Z}$ which is a solution to the system of simultaneous congruences*

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ldots, x \equiv a_2 \pmod{n_k}$$

and this solution is unique modulo $N = n_1 n_2 \ldots n_k$.

In order to prove this, one defines $N_i = N/n_i$ (which is the product of all of $n_1, \ldots, n_k$, except with n_ii removed from the product). Then $\text{hcf}(N_i, n_i) = 1$, so that there exists $\lambda_i, \mu_i \in \mathbb{Z}$ such that $\lambda_i N_i + \mu_i n_i = 1$, and so $\lambda_i N_i \equiv 1 \pmod{n_i}$. Then one can easily check that $x = \sum_{i=1}^k \lambda_i N_i a_i$ is a solution to the above system. If also y were a solution, then $x \equiv y \pmod{n_i}$ and so $n_i|(x-y)$ for all i; since $n_1, \ldots, n_k$ are pairwise coprime, this gives $N = n_1 n_2 \ldots n_k|(x-y)$, so that $x \equiv y \pmod N$; in other words, x is unique mod N, as required.

Another natural problem in Number Theory is that of trying to decide when one number is congruent to a square modulo a prime.

Definition 0.58. Let p be prime and $m \in \mathbb{Z}$. We say that m is a *quadratic residue* mod p if there exists $x \in \mathbb{Z}$ such that $m \equiv x^2 \pmod{p}$. Otherwise m is a *quadratic non-residue* mod p.

For example, consider what happens modulo $p = 5$. Every number is congruent to one of $0, 1, 2, 3$ or $4 \pmod 5$ [which are the same as $0, 1, 2, -2, -1 \pmod 5$]. Now: $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 = (-2)^2 \equiv 4, 4^2 = (-1)^2 \equiv 1 \pmod 5$. So, $0, 1, 4$ are quadratic residues mod 5, but $2, 3$ are not.

Lemma 0.59. *For any prime $p \neq 2$, let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, with addition and multiplication mod p, and let $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$, the nonzero elements of $\mathbb{Z}_p$. Define $\psi : \mathbb{Z}_p^* \to \mathbb{Z}_p^* : x \mapsto x^2$ is a 2-to-1 map [2 elements map to 1 element], with $\psi(x) = \psi(p-x)$, or equivalently $\psi(x) = \psi(-x)$ [since $(p-x)^2 \equiv (-x)^2 \equiv x^2 \pmod p$]. So exactly half of $\{1, \ldots, p-1\}$ are quadratic residues mod p and half are quadratic non-residues mod p.*

Definition 0.60. For prime p and $p \nmid m$, define the *Legendre symbol* by:

$$\left(\tfrac{m}{p}\right) = \begin{cases} 1 & \text{if } m \text{ is a quadratic residue mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

When $p|m$, we normally define $\left(\frac{m}{p}\right) = 0$.

For example, we have already seen that $\left(\frac{2}{5}\right) = -1$. Also, $\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$, since 7 and 2 are congruent (mod 5). Similarly, $\left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$ and $\left(\frac{10}{5}\right) = 0$.

Lemma 0.61. *Let p be an odd prime and let $p \nmid m, n, m_1, m_2$.*
(a) *If $m_1 \equiv m_2 \pmod p$ then $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$.*
(b) $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$*, which is the same as saying:*
mn is a quadratic residue mod p $\iff$ either (m and n are both quadratic residues mod p) or (m and n are both quadratic non-residues mod p)
(c) $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4$ *or* $p = 2$. $\left(\frac{-1}{p}\right) = -1 \iff p \equiv 3 \pmod 4$.
(d) $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 8$. $\left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3 \pmod 8$.

Theorem 0.62. *(Gauss' Law of Quadratic Reciprocity). Let $p \neq 2, q \neq 2$ be distinct primes.*
If either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
If both $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$ then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Example 0.63. Let us decide whether 6 is a quadratic residue mod 1019 [which is prime], using applications of quadratic reciprocity.

$\left(\frac{6}{1019}\right) = \left(\frac{2}{1019}\right)\left(\frac{3}{1019}\right) = (-1)\left(\frac{3}{1019}\right)$ [by Lemma **??**(d)]
$= (-1)(-1)\left(\frac{1019}{3}\right)$ [by quadratic reciprocity, since both 1019 and 3 are $\equiv 3 \pmod 4$]
$= (-1)(-1)\left(\frac{2}{3}\right) = (-1)(-1)(-1) = -1$,

establishing that 6 is a quadratic non-residue mod 1019 [and so there does not exist an integer x such that $6 \equiv x^2 \pmod{1019}$], in a way much quicker than checking that none of $0^2, 1^2, \ldots, 1018^2$ are congruent to 6 (mod 1019).

Quadratic reciprocity also gives a quick way, for any given integer n, of describing all primes p such that n is a quadratic residue mod p.

Example 0.64. Let us describe the primes p for which 3 is a quadratic residue mod p. First note that 3 is a quadratic residue mod 2 and mod 3, so it remains to consider $p > 3$. For $p > 3$, p is divisible by neither 2 nor 3, and so $p \equiv 1$ or 3 mod 4 and $p \equiv 1$ or 2 mod 3. When we apply quadratic reciprocity to go from $\left(\frac{3}{p}\right)$ to $\left(\frac{p}{3}\right)$, the cases $p \equiv 1$ or 3 mod 4 will determine whether a negative sign is introduced. Then the value of $\left(\frac{p}{3}\right)$ will be determined by whether $p \equiv 1$ or 2 mod 3. So, it is natural to see what happens in each of the following four cases.
Case 1: $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$ [which is the same as: $p \equiv 1 \pmod{12}$]. In this case: $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ [by quadratic reciprocity] $\left(\frac{1}{3}\right)$ [since $p \equiv 1 \pmod 3$] $= 1$.
Case 2: $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 3$ [which is the same as: $p \equiv 5 \pmod{12}$]. In this case: $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{2}{3}\right) = -1$.
Case 3: $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$ [which is the same as: $p \equiv 7 \pmod{12}$]. In this case: $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) - \left(\frac{1}{3}\right) = -1$.
Case 4: $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$ [which is the same as: $p \equiv 11 \pmod{12}$]. In this case: $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) - \left(\frac{2}{3}\right) = -(-1) = 1$.

To summarise: 3 is a quadratic residue mod $p \iff p = 2, p = 3$ or $p \equiv 1, 11 \pmod{12}$.

Rings

There are many situations where we have two operations on the same set, for example $\mathbb{Z}$ with both addition and multiplication.

Definition 0.65. Let R have two binary operations $+, \times$. R is a *ring* (with 1) if:

R is a commutative group under $+$ with identity 0.

There exists an element 1 ($\neq 0$) such that, for all $r \in R$, $1 \times r = r \times 1 = r$.

For all $r, s, t \in R$, $(r \times s) \times t = r \times (s \times t)$ [associativity of multiplication].

For all $r, s, t \in R$, $r \times (s + t) = r \times s + r \times t$, $(s + t) \times r = s \times r + t \times r$ [left and right distributivity].

Note that, for any ring, addition is always commutative, but multiplication need not be commutative. When multiplication is commutative [that is, $r \times s = s \times r$ for all $r, s \in R$] we say that R is a *commutative ring*.

Examples 0.66.
(a) $\mathbb{Z}, +, \times$ is a commutative ring.
(b) For any ring R, define $R[x] = \{\text{polynomials in } x \text{ with coefficients in } R\}$, which is also a ring, with the usual addition and multiplication of polynomials. Also define the ring $R[[x]] = \{\text{power series in } x \text{ with coefficients in } R\}$. The same is true when there are several variables, for example: $R[x, y], R[[x, y]]$.
(c) Let $G, +$ be any commutative group. Let $\mathrm{End}(G) = \{\phi : \phi \text{ is an endomorphism on } G\}$. Then $\mathrm{End}(G)$ is a ring, with operations: $(\phi_1 + \phi_1)(g) = \phi_1(g) + \phi_2(g)$ [defining ring addition $\phi_1 + \phi_2$], and with ring multiplication given by $\phi_1 \circ \phi_2$ [composition]. This is the *endomorphism ring* of the group G.
(d) $M_2(\mathbb{Z}) = \{2 \times 2 \text{ matrices with integer entries}\}$ is a non-commutative ring, with '0' given by $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and '1' given by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
(e) The set $\{0, \ldots, n-1\}$ under addition and multiplication modulo n is a commutative ring.

Definition 0.67. Let R, S be rings. Define the ring $R \times S = \{(r, s) : r \in R, s \in S\}$ with $+$ and $\times$ on $R \times S$ defined by:

$(r_1, s_1) + (r_2, s_2) = (r_1 +_R r_2, s_1 +_S s_2)$, $\quad (r_1, s_1) \times (r_2, s_2) = (r_1 \times_R r_2, s_1 \times_S s_2)$, where $+_R, +_S$ denote addition in R, S, respectively, and where $\times_R, \times_S$ denote multiplication in R, S, respectively.

Definition 0.68. A commutative ring R is an *integral domain* if, for all $r, s \in R$,

$$rs = 0 \implies (r = 0 \text{ or } s = 0).$$

For example, $\mathbb{Z}$ and $\mathbb{Z}[[x]]$ are integral domains, but $M_2(\mathbb{Z})$ is not, since $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Definition 0.69. Let R, S be rings. A function $\phi : R \to S$ is a *ring homomorphism* if, for all $r_1, r_2 \in R$, $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 \times r_2) = \phi(r_1) \times \phi(r_2)$. Define the *kernel* as $\ker \phi = \{r \in R : \phi(r) = 0\}$ and the *image* as $\mathrm{im}\, \phi = \{\phi(r) : r \in R\}$. If ϕ is also injective then ϕ is a *monomorphism* (or *embedding*). If ϕ is also a bijection, then ϕ is a *ring isomorphism*.

If there exists an isomorphism from R to S, then R and S are *isomorphic*, denoted $R \cong S$.

The equivalent idea for rings to that of normal subgroups is as follows.

Definition 0.70. An *ideal* of a ring R is a subset $I \subset R$ satisfying:
$I, +$ is a subgroup of $R, +$.
For all $r \in R, a \in I$ we have $r \times a \in I$ and $a \times r \in I$.
We sometimes use $I \lhd R$ to denote that I is an ideal of R.

This last condition can be phrased as: 'the product of anything in the ring with anything in the ideal must be in the ideal'. Note that $1 \in I \iff I = R$. If $I \neq R$ then I is

a *proper ideal*. If I is a proper ideal and is not contained in a larger proper ideal, then I is a *maximal ideal*. We say that J is a *prime ideal* if it is a proper ideal and: for all a, b, if $ab \in J$ then $a \in J$ or $b \in J$. Given any $a_1, \ldots, a_n \in R$, we use $(a_1, \ldots, a_n)$ to denote $\{r_1a_1 + \ldots + r_na_n : r_i \in R\}$, which is the *ideal generated by* $a_1, \ldots, a_n$. An ideal generated by one element a, namely an ideal which can be written in the form $(a) = \{ra : r \in R\}$ is called a *principal ideal*.

Given two ideals I, J of R, the intersection $I \cap J$ is an ideal of R; we define $I + J = \{a+b : a \in I, b \in J\}$, which is also an ideal of R. We have to be more careful with IJ, since $\{ab : a \in I, b \in J\}$ is not always an ideal, so we instead define IJ to be the ideal generated by these products, that is to say, we define $IJ = \left\{\sum_{i=1}^{k} a_ib_i : a_i \in I, b_i \in J, k \geqslant 1\right\}$, which is an ideal of R. Note that always $IJ \subseteq I \cap J \subseteq I, J \subseteq I + J$.

Definition 0.71. Let I be an ideal of a ring R; define the quotient ring $R/I = \{r+I : r \in R\}$, under the operations $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ and $(r_1 + I) \times (r_2 + I) = (r_1 \times r_2) + I$.

Note that I is an ideal if and only if it occurs as the kernel of a ring homomorphism from R to some ring.

Lemma 0.72. *Let R be a commutative ring. Then I is a prime ideal of R if and only if R/I is an integral domain.*

For example, $x\mathbb{Z}[x]$ [the polynomials with 0 constant term] is an ideal of the ring $\mathbb{Z}[x]$ (and it is a principal ideal (x)). It is a prime ideal, so that $\mathbb{Z}[x]/(x)$ must be an integral domain. It is the kernel of the ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}$, defined by $p(x) \mapsto p(0)$. Furthermore: $\mathbb{Z}[x]/x\mathbb{Z}[x] \cong \mathbb{Z}$. Similarly, for any fixed n, clearly $n\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$ (and is the principal ideal (n)); the ring of Example **??**(e) is just the quotient ring $\mathbb{Z}/n\mathbb{Z}$. Note that $n\mathbb{Z}$ is a prime ideal if and only if n is prime. Hence $\mathbb{Z}/n\mathbb{Z}$ (which is just the ring $\{0, \ldots, n-1\}$ under addition and multiplication modulo n) is an integral domain if and only if n is prime.

Warning. An ideal can still be principal even if it not initially expressed in terms of one generator. For example, consider the ideal $I = (4, 6)$, which is (by definition) the ideal of $\mathbb{Z}$ generated by 4 and 6, so that $I = (4, 6) = \{4r_1 + 6r_2 : r_1, r_2 \in \mathbb{Z}\}$. Note that $2 = 4 \times \{-1\} + 6 \times 1 \in I$ so that any $2 \times r \in I$ and so: $(2) \subseteq I$. Also any $4r_1 + 6r_2 \in I$ can be written as $2\{2r_1 + 3r_2\} \in (2)$. Hence $I = (2)$. So, $I = (4, 6)$ is a principal ideal, since it can also be written as (2).

Rings have isomorphism theorems similar to those for groups (and the proofs are similar).

Theorem 0.73. *[First Isomorphism Theorem for Rings] Let R, S be rings and $\phi : R \to S$ be a ring homomorphism. Then* $\ker \phi \lhd R$*, im ϕ is a subring of R and* $R/\ker \phi \cong$ *im ϕ. In particlar, if ϕ is surjective then* $R/\ker \phi \cong S$.

Theorem 0.74. *[Second Isomorphism Theorem for Rings] Let R be a ring, S be a subring of R and $I \lhd R$. Then $S + I = \{s + i : s \in S, i \in I\}$ is a subring of R, $S \cap I \lhd R$ and $(S + I)/I \cong S/(S \cap I)$.*

Theorem 0.75. *[Third Isomorphism Theorem for Rings] Let R be a ring and let $I, J \lhd R$ with $I \subseteq J \subseteq R$. Then $J/I \lhd R/I$ and $(R/I)/(J/I) \cong R/J$.*

Definition 0.76. Let R be a ring. If there exists an integer $n \geqslant 1$ such that $1 + 1 + \ldots + 1[n \text{ times}] = 0$, then the smallest such n is the *characteristic* of R. If no such n exists, then R is said to have characteristic 0.

For example, $\mathbb{Z}/n\mathbb{Z}$ has characteristic n, whereas $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ all have characteristic 0.

Suppose that I is a maximal ideal of some commutative ring R. Imagine it were not a prime ideal, so that there exist $r, s \in I$ such that $rs \in I$ but $r, s \notin I$. Define $\langle I, r\rangle = \{a + rt \mid a \in I, t \in R\}$ and $\langle I, s\rangle = \{a + st \mid a \in I, t \in R\}$. Clearly $I \subset \langle I, r\rangle$ and $I \neq \langle I, r\rangle$ (since $r \in \langle I, r\rangle$ and $r \notin I$), so that $\langle I, r\rangle = R$ (since I is maximal); hence (since $1 \in R$) there exist $a \in I, t \in R$ such that $1 = a + rt$. Similarly there exist $a' \in I, t' \in R$ such that $1 = a' + st'$. Hence $1 = (a + rt)(a' + st') = aa' + ast' + a'rt + rstt' \in I$, since I is an ideal (and since $a, a', rs \in I$). But $1 \in I$ gives, for any $r \in R$ that $r = r \times 1 \in I$ so that $I = R$, contradicting the maximality of I. This proves the following result.

Theorem 0.77. *Let R be a commutative ring. Every maximal ideal of R is a prime ideal of R.*

The converse is false; for example, $(x) = x\mathbb{Z}[x]$ is a prime ideal of the ring $\mathbb{Z}[x]$ but it is not a maximal ideal since, for example, $(x) \subseteq (2, x) \subseteq \mathbb{Z}[x]$ (all of which are strict inequalities), where $(2, x)$ is the ideal generated by 2 and x (which is the set of all polynomials in $\mathbb{Z}[x]$ with even constant term).

Definition 0.78. Two ideals I, J of a ring R are *coprime* if $I + J = R$.

For example, the ideals $m\mathbb{Z}$ and $n\mathbb{Z}$ of the ring $\mathbb{Z}$ are coprime ideals exactly when m, n are coprime integers, that is, when $\text{hcf}(m, n) = 1$. To see this, note that, when $\text{hcf}(m, n) = 1$, there exist $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = 1$ and so $1 = m\lambda m + n\mu \in m\mathbb{Z} + n\mathbb{Z}$ and so $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. If $\text{hcf}(m, n) = d > 1$ then clearly and $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z} \neq \mathbb{Z}$.

Theorem 0.79. *[Chinese Remainder Theorem (for rings)] Let R be a commutative ring and let $I_1, \ldots, I_k$ be ideals of R which are pairwise coprime (that is, $I_i + I_j = R$ whenever $i \neq j$). Let $I = I_1 \cap I_2 \cap \ldots \cap I_k$. Then $I = I_1 I_2 \cdots I_k$ (the product equals the intersection) and $R/I \cong R/I_1 \times \ldots \times R/I_k$ under the natural isomorphism $\phi : R/I \to R/I_1 \times \ldots R/I_k$ given by $\phi(x + I) = (x + I_1, \ldots, x + I_k)$.*

The earlier Chinese Remainder Theorem (for congruences) is a special case of this. Suppose that we have the system

$$x \equiv a_1 \pmod{n_1},\ x \equiv a_2 \pmod{n_2},\ \ldots\ ,\ x \equiv a_k \pmod{n_k},$$

with $n_1, \ldots, n_k$ pairwise coprime integers, and let $N = n_1 n_2 \ldots n_k$. Then $n_1\mathbb{Z}, \ldots, n_k\mathbb{Z}$ are pairwise coprime ideals of the ring $\mathbb{Z}$ and the Chinese Remainder Theorem (for rings) tells us that $I = n_1\mathbb{Z} \cap n_2\mathbb{Z} \cap \ldots \cap n_k\mathbb{Z} = n_1\mathbb{Z}n_2\mathbb{Z}\cdots n_k\mathbb{Z} = N\mathbb{Z}$ and that $\phi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$, given by $\phi(x + N\mathbb{Z}) = (x + n_1\mathbb{Z}, \ldots, x + n_k\mathbb{Z})$, is an isomorphism. Hence there is a unique $x + N\mathbb{Z} \in \mathbb{Z}/N\mathbb{Z}$ which maps to $(a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z})$, which is precisely the same as saying there there is a unique solution (mod N) to the above system of congruences.

Now, let R be any commutative ring and $I \lhd R$. If $J \lhd R$ and $I \subseteq J \subseteq R$ then $J/I \lhd R/I$ and so the map $\phi : J \mapsto J/I$ gives a map from the set $\{J : J \lhd R \text{ and } I \subseteq J \subseteq R\}$ to the set $\{V : V \lhd R/I\}$. In the reverse direction, if $V \lhd R/I$ then $\{r \in R : r + I \in V\} \lhd R$. It can be shown that the map $\psi : V \mapsto \{r \in R : r + I \in V\}$ is the inverse of ϕ which gives the following result.

Theorem 0.80. *Let R be a commutative ring and let $I \lhd R$. Then there is a 1-1 correspondence between the set of ideals of R containing I and the set of ideals of R/I.*

It can also be shown that primality is preserved, and so there is also a 1-1 correspondence between the set of prime ideals of R containing I and the set of prime ideals of R/I.

Definition 0.81. Let R be a commutative ring. We say that $a|b$ (*a divides b*) in R if there exists $c \in R$ such that $b = ac$. The element $u \in R$ is a *unit* if $u|1$, that is, if there exists $v \in R$ wuch that $uv = 1$. We say that a, b are *associates* if there exists a unit u such that $b = au$. An element $d \in R$ is called a *highest common factor* of a, b if $d|a,\ d|b$ and if, for any $c \in R$, $(c|a,\ c|b) \implies c|d$. Note that, for a general commutative ring and general elements a, b, there might not even exist such and element d (when such an element does exist, it is clearly unique up to multiplication by units). An non-zero non-unit element $\rho \in R$ is *irreducible* if, for any $a, b \in R$, $\rho = ab \implies a$ or b is a unit. An non-zero non-unit element $\rho \in R$ is *prime* if, for any $a, b \in R$, $\rho|ab \implies \rho|a$ or $\rho|b$.

If ρ is prime then by induction, $\rho|a_1a_2 \ldots a_n \implies \rho|a_i$ for some i.

Warning: the definition of prime (in $\mathbb{Z}$) which you were given in school is actually the definition of irreducible! In any case, as we shall see, primes and irreducibles in $\mathbb{Z}$ turn out to be the same.

It is easy to show that, in any integral domain, every prime element must be irreducible, but the converse is false; for example, in the ring $\mathbb{Z}[\sqrt{-5}]$ the element 2 is irreducible but not prime (since $2|(1+\sqrt{-5})(1-\sqrt{-5})$ even though $2 \nmid 1+\sqrt{-5}$ and $2 \nmid 1-\sqrt{-5}$).

One of the central problems in ring theory is to determine whether or not a given ring has unique factorisation into irreducibles. If one thinks for a moment how to show this for $\mathbb{Z}$, a quick summary of one line of argument is as follows. First (by induction) prove the Division Algorithm that, for any $a, b \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $|r| < |b|$. Now let $0 \neq I \lhd \mathbb{Z}$, and let d be the smallest positive member of I; then $I = (d)$ (otherwise the Division Algorithm would give a smaller positive member of I). Hence every ideal of $\mathbb{Z}$ is a principal ideal. For any $m, n \in \mathbb{Z}$, the ideal $(m, n) = m\mathbb{Z} + n\mathbb{Z}$ must be principal, say that $m\mathbb{Z} + m\mathbb{Z} = c\mathbb{Z}$; it is easy to show that c is a highest common factor of m, m and that there exist $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = c$. Suppose that $\rho \in \mathbb{Z}$ is irreducible. Assume $\rho|ab$ and $\rho \nmid a$; let c be a highest common factor of ρ, a (which we have just shown exists); then c must be a unit, and we can take $c = 1$, so there exist $\lambda, \mu \in \mathbb{Z}$ such that $\lambda\rho + \mu a = 1$, and so: $\lambda\rho b + \mu ab = b$. Then $\rho|LHS$ and so $\rho|b$, proving that ρ is prime. Hence, in the ring $\mathbb{Z}$, primes and irreducibles are the same.

Imagine there exists $n \in \mathbb{Z}$ which cannot be factored as a product of a finite number of irreducibles. Then we can write $n = n_1 a_1$, $n_1 = n_2 a_2$, ..., say, where none of the n_i, a_i are units, and so we can find an infinite sequence $n_1, n_2, \ldots$ such that each $n_{i+1}|n_i$ and $n_i \nmid n_{i+1}$. This gives a chain of ideals: $n_1\mathbb{Z} \subset n_2\mathbb{Z} \subset \ldots$, where each $n_i\mathbb{Z} \neq n_{i+1}\mathbb{Z}$. Let $I = \bigcup_{i=1}^{\infty} n_i\mathbb{Z}$, which can easily be shown to be an ideal of $\mathbb{Z}$; since all ideals of $\mathbb{Z}$ are principal, there must exist $m \in \mathbb{Z}$ such that $I = m\mathbb{Z}$ and furthermore $m \in n_{i_0}\mathbb{Z}$, for some n_{i_0}. It is then quick to show that $n_{i_0}\mathbb{Z} = n_{i_0+1}\mathbb{Z} = \ldots$, a contradiction. Hence every $n \in \mathbb{Z}$ can be factored as a product of a finite number of irreducibles.

Imagine such factorisations were not always unique and that there exists $\rho_1\rho_2 \ldots \rho_r = \nu_1\nu_2 \ldots \nu_s$, where all ρ_i, ν_j are irreducible and where the RHS cannot be obtained from the LHS merely by reordering and replacing elements with associates. Amongst all such non-unique factorisations, consider one such for which $r + s$ is minimal. We have already seen that all irreducibles are prime, so that ρ_1 is prime. Furthermore, $\rho_1|\nu_1\nu_2 \ldots \nu_s$, so that $\rho_1|\nu_j$ for some j; without loss of generality, say that $\rho_1|\nu_1$. It follows that ρ_1, ν_1 are associates. On cancelling ρ_1 from both sides, one has a new example of non-unique factorisation, but with a smaller value of $r + s$, a contradiction. Hence factorisation is unique.

It should be confessed here that the above is a rather convoluted approach simply for showing that $\mathbb{Z}$ has unique factorisation and there are a number of shortcuts available which work for $\mathbb{Z}$. For example, Euclid's Algorithm (and reversing the steps of Euclid's Algorithm) gives the existence of $\text{hcf}(m, n)$ and the fact that it can be written as $\lambda m + \mu n$. Furthermore

the mere existence of a factorisation into a product of a finite number of irreducibles can be proved (for $\mathbb{Z}$) by induction. However, it is the above style of argument which is a amenable to generalisation to a wider class of rings.

In the above the Division Algorithm allowed us to deduce that all ideals in $\mathbb{Z}$ are principal which in turn allowed us to deduce unique factorisation (and there was a step which involved cancelling a nonzero element from both sides of an equation, which used that fact that $\mathbb{Z}$ is an integral domain). So, it seems reasonable to define a natural generalisation of the Division Algorithm which might apply to a wider class of rings.

Definition 0.82. Let R be an integral domain. R is a Euclidean domain (ED) if and only if there exists a function (a *Euclidean function*) $d : R\backslash\{0\} \to \mathbb{N} \cup \{0\}$ such that

(i) For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $d(r) < d(b)$.

(ii) For all nonzero $a, b \in R,\ d(a) \leqslant d(ab)$.

Definition 0.83. Let R be an integral domain. R is a principal ideal domain (PID) if and only if every ideal is principal (that is, every ideal is of the form $(\gamma) = \{r\gamma : r \in R\}$).

Definition 0.84. Let R be an integral domain. R is a unique factorisation domain (UFD) if and only if for all non-zero and non-unit $\alpha \in R$ there exist irreducible $\beta_1, \ldots, \beta_n \in R$ such that

(i) $\alpha = \beta_1 \ldots \beta_n$

(ii) If $\alpha = \gamma_1 \ldots \gamma_m$ with irreducible γ_i, then $m = n$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that β_i and $\gamma_{\sigma(i)}$ are associates.

The following theorem is proved by imitating the argument given above for $\mathbb{Z}$.

Theorem 0.85. *ED* $\implies$ *PID* $\implies$ *UFD.*

Example 0.86. As we have seen, $\mathbb{Z}$ has Euclidean function $d(n) = |n|$. Similarly, it can be shown that $d(a+bi) = a^2+b^2$ is a Euclidean function on the ring $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$. It can also be shown that $d(p(x)) = \text{degree}(p(x))$ is a Euclidean function on $\mathbb{Q}[x]$ and indeed on any $K[x]$, where K is any field (see below for the definition of field); this uses the polynomial division algorithm (giving a remainder polynomial with strictly smaller degree). So, all of $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Q}[x], K[x]$ (for any field K) are examples of ED (and so also PID and UFD).

Note however that $\mathbb{Z}[x]$ is *not* an ED (the polynomial divisional algorithm does not work here; try, for example, dividing $2x + 3$ into $3x^2 + 7$, while using only elements of $\mathbb{Z}[x]$). Indeed one can prove that it is not an ED by showing that it is not a PID: consider the ideal generated by $2, x$, namely: $(2, x) = \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]]\}$ (the set of

polynomials in $\mathbb{Z}[x]$ with even constant term); this can be shown not to be a principal ideal. On the other hand, $\mathbb{Z}[x]$ is still a UFD.

The ring $\mathbb{Z}[\sqrt{-5}]$ is not even a UFD, as we can see from $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$; one can check that $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducible and no two of them are associates.

Fields

Definition 0.87. Let K have two binary operations $+, \times$. K is a *field* if:

K is an Abelian group under $+$ with identity 0,

The nonzero elements of K is an Abelian group under $\times$ with identity 1,

For all $a, b \in K$, $a \times (b + c) = a \times b + a \times c$ [distributivity].

Equivalently, we could define a field to be a commutative ring for which every nonzero element has a multiplicative inverse.

Theorem 0.88. *Let R be a finite integral domain. Then R is a field.*

Proof Let $R = \{r_1, \ldots, r_n\}$ be the distinct elements of R. It is sufficient to show that all nonzero elements have multiplicative inverses. Let $a \in R$ be nonzero. Consider the set $\{ar_1, \ldots, ar_n\}$. Note that: $ar_i = ar_j \implies a(r_i - r_j) = 0 \implies r_i - r_j = 0$ (since $a \neq 0$ and R is an integral domain), which is only possible when $i = j$ (since $r_1, \ldots, r_n$ are distinct). Hence $ar_1, \ldots, ar_n$ are distinct; there are n of these, so they must give all n elements of R by the pigeonhole principle. Since $1 \in R$ there must exist $r_i \in R$ such that $ar_i = 1$, and so a has a multiplicative inverse, as required. □

Examples 0.89.

(a) $\mathbb{Q}, +, \times$ is a field.

(b) Let $\mathbb{Z}_p, +, \times$ denote $\{0, 1, \ldots, p-1\}$ under addition and multiplication modulo p, where p is prime [this is the same as $\mathbb{Z}/p\mathbb{Z}, +, \times$]. This a field with p elements (a *finite field*, since it has only finitely many elements, as opposed to the infinite field $\mathbb{Q}$). The fact that it is a group under addition modulo p is straightforward. The fact that the nonzero elements form a group under multiplication modulo p was shown in Corollary **??**

(c) $\mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$ are all fields. By $\mathbb{Q}(\sqrt{2})$ we mean $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, and similarly for $\mathbb{Q}(i)$.

(d) $\mathbb{Z}, +, \times$ is not a field since the nonzero integers is not a group under multiplication (for example, 3 has no inverse under multiplication).

(e) $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$ under addition and multiplication modulo 6 is not a field for the same reason.

(f) Let R be any commutative ring. Then $\mathcal{M}$ is a maximal ideal of R if and only if the quotient $R/\mathcal{M}$ is a field. Note that this gives an alternative method for showing that every

maximal ideal of R is a prime ideal of R, namely:

$$\mathcal{M} \text{ maximal} \iff R/\mathcal{M} \text{ is a field} \implies R/\mathcal{M} \text{ is an integral domain} \iff \mathcal{M} \text{ prime.}$$

(g) Given any integral domain R, define $K = \{\frac{a}{b} : a, b \in R, b \neq 0\}$, where we regard $\frac{a}{b} = \frac{a'}{b'}$ when $ab' = a'b$. This is the *field of fractions* of R. Addition and multiplication are defined as you would expect: $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 \times b_2 + a_2 \times b_1}{b_1 b_2}$ and $\frac{a_1}{b_1} \times \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$. More pedantically, you could define the field of fractions as $\{(a, b) : a, b \in R\}$ modulo the equivalence relation: $(a, b) = (a', b') \iff ab' = a'b$, with addition and multiplication defined by: $(a_1, b_1) + (a_2, b_2) = (a_1 \times b_2 + a_2 \times b_1, b_1 b_2)$ and $(a_1, b_1) \times (a_2, b_2) = (a_1 a_2, b_1 b_2)$. For example, $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. Also, $\mathbb{Q}(i)$ is the field of fractions of $\mathbb{Z}[i]$. In general, if R is an integral domain and $R \subseteq K$, where K is a field and if, for all *alpha* $\in K$, there exist $a, b \in R$ such that $\alpha = a/b$, then K must be the field of fractions of R.

(h) For any integral domain R, the field of fractions of $R[x]$ is denoted $R(x)$; it is the field of *rational functions* in x over R, that is, $R(x) = \{\frac{p(x)}{q(x)} : p(x), q(x) \in \mathbb{Z}[x], q(x) \neq 0\}$. Note that, if K is the field of fractions of R, then $R(x) = K(x)$.

Sometimes the field of fractions of an integral domain R (or indeed any field K containing R, which must therefore contain the field of fractions of R) can be used useful in trying to show that R is a ED, particularly when the proposed function d is multiplicative.

Lemma 0.90. *Let $R \subseteq K$, where R is an integral domain and K is a field. Suppose there exists a function $d : K \to \mathbb{Q}$, with $d(a) = 0 \iff a = 0$, and restriction $d : R \to \mathbb{N} \cup \{0\}$, with the properties that*

(i) *For any $\gamma \in K$, there exists $q \in R$ with $d(\gamma - q) < 1$.*

(ii) *For all nonzero $\alpha, \beta \in K$, $d(\alpha\beta) = d(\alpha)d(\beta)$.*

Then d is a Euclidean function on R.

Proof For any nonzero $a, b \in R$, $d(a), d(b) \in \mathbb{N}$ and so $d(ab) = d(a)d(b) \geqslant d(a)$, giving property (ii) of Definition **??**. Now let $a, b \in R$ with $b \neq 0$, and let $\gamma = a/b \in K$. By our assumption, there exists $q \in R$ with $d(\gamma - q) < 1$, so that $d(a/b - q) < 1$, and so $d(a - bq) = d((a/b - q)b) = d(a/b - q)d(b) < d(b)$. Let $r = a - bq \in R$. Then $a = bq + r$ and $d(r) < d(b)$, giving property (i) of Definition **??**. Hence d is a Euclidean function, as required. □

Example 0.91. Let $K = \mathbb{Q}(i)$ and $R = \mathbb{Z}[i]$. For any $\alpha = \alpha_1 + \alpha_2 i \in \mathbb{Q}(i)$ (where $\alpha_1, \alpha_2 \in \mathbb{Q}$), define $d : \mathbb{Q}(i) \to \mathbb{Q}$ by $d(\alpha_1 + \alpha_2 i) = (\alpha_1 + \alpha_2 i)(\alpha_1 - \alpha_2 i) = \alpha_1^2 + \alpha_2^2$. Clearly, $d : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$, $d(\alpha) = 0 \iff \alpha = 0$ and $d(\alpha\beta) = d(\alpha)d(\beta)$ for any $\alpha, \beta \in \mathbb{Q}(i)$. Let $\gamma = \gamma_1 + \gamma_2 i \in \mathbb{Q}(i)$, where $\gamma_1, \gamma_2 \in \mathbb{Q}$. Let q_1 be the closets integer to γ_1 and let q_2 be the closest integet to γ_2. Then $|\gamma_1 - q_1|$, $|\gamma_2 - q_2| \leqslant 1/2$ (since there is always an integer

distance at most 1/2 from any real number). Then $d(\gamma - q) = d((\gamma_1 - q_1) + (\gamma_2 - q_2)i)$ $= (\gamma_1 - q_1)^2 + (\gamma_2 - q_2)^2 \leqslant (1/2)^2 + (1/2)^2 = 1/2 < 1$, as required.

Since fields are special cases of rings, the definitions for field homomorphism, field isomorphism and characteristic are exactly as described for rings. An isomorphism from a field to itself is an *automorphism*.

Definition 0.92. Let $K, +, \times$ be a field. Then K^* always denotes the group of nonzero elements of K under $\times$ [for example, $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ are all groups under $\times$].

Definition 0.93. Let K be a field. Any $p(x) \in K[x]$ is *irreducible* if it cannot be written as a product of two polynomials in $K[x]$ both of degree $\geqslant 1$. It is *monic* if the leading coefficient [that is, the coefficient of the highest power of x] is 1. Let α be the root of any $p(x) \in K[x]$ (not necessarily irreducible); then α is *algebraic* over K. For example, $\sqrt{2}$ is algebraic over $\mathbb{Q}$, since it is a root of $x^2 - 2$; on the other hand, $\sqrt{\pi}$ is algebraic over $\mathbb{R}$, but can be shown not to be algebraic over $\mathbb{Q}$. Given any α, algebraic over K, there always exists monic $m_\alpha(x) \in K[x]$ of smallest degree n which has α as a root; this has the property that it is a factor of any other member of $K[x]$ which has α as a root. We say that $m_\alpha(x)$ is the *minimal polynomial* of α and that α is *algebraic of degree* n over K. The set of roots of $m_\alpha(x)$ are the *conjugates* of α over K. A field K is *algebraically closed* if every polynomial $p(x) \in K[x]$ contains a root in K.

For example, $\mathbb{C}$ is algebraically closed, but $\mathbb{Q}$ is not. For any field K (whether algebraically closed or not), there exists a field $\overline{K}$, the *algebraic closure* of K, which is the smallest algebraically closed field containing K. Given α, algebraic of degree m_α over K, we can form the field $K(\alpha)$, which is the smallest subfield of $\overline{K}$ containing K and α. We say that $K(\alpha)$ is the field obtained by *adjoining* α to K. A similar definition applied for any $K(\alpha_1, \ldots, \alpha_n)$. A field L is an *algebraic extension* of K if $K \subset L$ and every $\ell \in L$ is algebraic over K, otherwise L is a *transcendental* extension of K.

Examples 0.94.
(a) $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.
(b) The minimal polynomial of i over $\mathbb{Q}$ is $x^2 + 1$, so that i is algebraic of degree 2 over $\mathbb{Q}$, and $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

Lemma 0.95 (Gauss's Lemma)**.** *Let $p(t) \in \mathbb{Z}[t]$ be irreducible in $\mathbb{Z}[t]$; then it is also irreducible in $\mathbb{Q}[t]$.*

Proof. The broad strategy is to imagine $p(t)$ were reducible over $\mathbb{Q}$, with $p(t) = g(t)h(t)$ where $g(t), h(t) \in \mathbb{Q}[t]$, and then show there exists $\lambda \in \mathbb{Q}$, $\lambda \neq 0$, such that $\lambda g, \lambda^{-1} h \in \mathbb{Z}[t]$ (the existence of such λ is sometimes included in the statement of Gauss' Lemma). $\square$

Theorem 0.96 (Eisenstein)**.** *Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$. Suppose there exists a prime p such that p does not divide a_n, but p divides a_i for $i = 0, \ldots, n-1$, and p^2 does not divide a_0. Then, apart from constant factors, $f(t)$ is irreducible over $\mathbb{Z}$, and hence irreducible over $\mathbb{Q}$.*

Such a polynomial is said to be Eisenstein with respect to the prime p. Note also: *irreducible over K* is just another way of saying: irreducible in $K[t]$

Proof It is quite a common first reaction to regard the Eisenstein condition as rather whimsical and arbitrary. For any $f(t)$ as above, let $\tilde{f}(t)$ denote $\tilde{a}_0 + \tilde{a}_1 t + \ldots + \tilde{a}_n t^n$, where all coefficients $a_i \in \mathbb{Z}$ are replaced with $\tilde{a}_i \equiv a \pmod{p}$, so that each $\tilde{a}_i \in \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. The most natural approach is first to assume that $f(t)$ is reducible, say $f(t) = g(t)h(t)$, where $g(t), h(t)$ have degrees k, ℓ, respectively, so that $k + \ell = n$. Assume also that $\tilde{f}(t) = \tilde{a}_n t^n$, with $\tilde{a}_n \neq 0$ (that is, only the leading term remains), which is equivalent to: p does not divide a_n, but p divides a_i for $i = 0, \ldots, n-1$. Note that $\tilde{f}(t) = \tilde{a}_n t^n$ is already expressed as a unit in $\mathbb{Z}_p[t]$ (namely $\tilde{a}_n$) times a product of irreducibles in $\mathbb{Z}_p[t]$ (namely each t) and so this must already be the unique factorisation of $\tilde{f}(t)$, since $\mathbb{Z}_p[t]$ is a UFD (recall that the ring $K[t]$ is a ED for any field K and so is a PID and UFD). But $\tilde{f}(t) = \tilde{g}(t)\tilde{h}(t)$, so by uniqueness of factorisation, $\tilde{g}(t)$ and $\tilde{h}(t)$ must also just consist of their leading terms. In particular, the constant terms of $g(t)$ and $h(t)$ must both be divisible by p, so that the a_0 (the product of these) must be divisible by p^2. To summarise, we have shown that if $f(x)$ is reducible in $\mathbb{Z}[x]$ and p does not divide a_n, but p divides a_i for $i = 0, \ldots, n-1$, then $p^2 | a_0$. Hence, if Eisenstein's Criterion is satsfied then $f(x)$ is irreducible in $\mathbb{Z}[x]$. □

Example 0.97. Let γ satisfy $x^3 - 2 = 0$. This is irreducible over $\mathbb{Z}$ by Eisenstein's Criterion (with $p = 2$) and so is irreducible over $\mathbb{Q}$ by Gauss' Lemma. Hence $x^3 - 2$ must be the minimal polynomial for γ over $\mathbb{Q}$.

Definition 0.98. Let L be a field extension of K [that is, K, L are fields and $K \subset L$; this is sometimes denoted L/K]. If there exists a finite set $\ell_1, \ldots, \ell_n \in L$ such that every $\ell \in L$ can be written as $\ell = k_1\ell_1 + \ldots + k_n\ell_n$, for some $k_1, \ldots, k_n \in K$, then L is a *finite extension* of K. In such cases, it is then always possible to find such a set with the extra property that $k_1\ell_1 + \ldots + k_n\ell_n \neq 0$ except when $k_1 = \ldots = k_n = 0$, in which case we say that $\ell_1, \ldots, \ell_n$ is a *basis* for the field extension. We then say that n is the *degree* of the extension $L : K$, or that $[L : K] = n$. Of course, if you wish, you can also phrase this in terms of vector spaces. Letting the set of vectors be L and the field of scalars be K, then L forms a vector space with respect to vector addition: $\ell_1 + \ell_2$, for any $\ell_1, \ell_2 \in L$, being simply the usual addition in the field L, and scalar multiplication $k\ell$, for any $k \in K, \ell \in L$, being simple the usual

multiplication in L. Then the degree of the extension $L : K$ is just the dimension of this vector space.

If α has minimal polynomial of degree n over K then $[K(\alpha) : K] = n$. For example, if γ satisfies $x^3 - 2 = 0$, we have already seen that this must be the minimal polynomial for γ and so $[\mathbb{Q}(\gamma) : \mathbb{Q}] - 3$.

A *algebraic number field* is a finite extension of $\mathbb{Q}$ (often this is just abbreviated to *number field*). For example, $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}, \sqrt{3})$ are all number fields. It can be shown that every number is expressible in the form $\mathbb{Q}(\alpha)$, for some α which is algebraic over $\mathbb{Q}$ (for example, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be shown to be the same as $\mathbb{Q}(\sqrt{2} + \sqrt{3})$).

Example 0.99. The field $\mathbb{Q}(\sqrt{2})$ is a degree 2 extension of $\mathbb{Q}$, with basis $1, \sqrt{2}$.

Theorem 0.100. *[Tower Theorem] Let $K \subset L \subset M$ be fields. Then:*

$$[M : K] = [M : L][L : K].$$

If $\ell_1, \ldots, \ell_r$ is a basis for L over K and $m_1, \ldots, m_s$ is a basis for M over L then the set of all $\ell_i m_j$, for $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s$, is a basis for M over K.

Definition 0.101. Let L be a field extension of K. Define the set

$$\mathrm{Aut}(L : K) = \{\sigma : L \to L : \sigma \text{ is an automorphism and } \sigma(k) = k \text{ for all } k \in K\},$$

that is, the set of all automorphisms of L which fix K [recall that an automorphism of L is a a field isomorphism from L to itself]. Then $\mathrm{Aut}(L : K)$ forms a group under the operation of function composition, the *automorphism group* of the extension $L : K$.

For any subgroup $H \leqslant \mathrm{Aut}(L : K)$, the *fixed field* of H is the field $\{\ell \in L : \sigma(\ell) = \ell \text{ for all } \sigma \in H\}$. If K is the fixed field of $\mathrm{Aut}(L : K)$, we say that $L : K$ is a *Galois extension* and we refer to $\mathrm{Aut}(L : K)$ as the *Galois group* of the extension, denoted $\mathrm{Gal}(L : K)$ or $\mathrm{Gal}(L/K)$ or $\mathrm{Gal}_{L/K}$.

Example 0.102. The group $\mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\big)$ has two elements: $\sigma_1 : a + b\sqrt{2} \mapsto a + b\sqrt{2}$ and $\sigma_2 : a + b\sqrt{2} \mapsto a - b\sqrt{2}$. This can be seen as follows. First note that, since σ is a field homomorphism, it fixes $\mathbb{Q}$. Also, $\sqrt{2}^2 - 2 = 0$ and taking σ of both sides give $\sigma(\sqrt{2}^2 - 2) = \sigma(0) = 0$, and so: $(\sigma(\sqrt{2}))^2 - 2 = 0$, which means that $\sigma(\sqrt{2})$ is a root of $x^2 - 2$, giving only two possibilities: $\sigma(\sqrt{2}) = \sqrt{2}$, when we must have $\sigma = \sigma_1$, or $\sigma(\sqrt{2}) = -\sqrt{2}$, when we must have $\sigma = \sigma_2$.

Definition 0.103. Let K be a field and let $f(x) \in K[x]$. The smallest field L containing K and all roots of $f(x)$ is called the *splitting field* of $f(x)$ over K.

It can be shown that, given any field K and any $f(x) \in K[x]$, there exists a splitting field of $f(x)$ over K.

Example 0.104. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and let γ be the real cube root of 2. Then $f(x) = (x-\gamma)(x-\omega\gamma)(x-\omega^2\gamma)$, where $\omega = e^{2\pi/3}$ satisfies $\omega^2 + \omega + 1 = 0$. It can be shown that the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\gamma, \omega)$, which is a degree 6 extension of $\mathbb{Q}$.

Definition 0.105. Let K, L be fields. An *embedding* (or *monomorphism*) of K into L is a map from K to L which is an injective homomorphism.

Lemma 0.106. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n over $\mathbb{Q}$, so that any member of K can be written as $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, for $\alpha_i \in \mathbb{Q}$. and let $f(x)$ be the minimal polynomial of $f(x)$ over $\mathbb{Q}$, with roots $\alpha_1, \ldots, \alpha_n$ (one of which is α itself). Let $\sigma : K \to \mathcal{C}$ be an embedding of K into $\mathcal{C}$, the complex numbers. By similar reasoning to Example **??**, σ fixes $\mathbb{Q}$ and must map α to α_i, for some i. Furthermore, this fixes the embedding, since then $\sigma(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \ldots + \sigma(a_{n-1})\sigma(\alpha)^{n-1} = a_0 + a_1\alpha_i + \ldots + a_{n-1}\alpha_i^{n-1}$. Hence there are precisely n embeddings of K into $\mathcal{C}$.*

We say that σ is a *real* embedding if it maps K into $\mathbb{R}$; otherwise we say that σ is a complex embedding (that is, if there exists $x \in K$ such that $\sigma(x) \notin \mathbb{R}$. It is standard notation here to let r denote the number of real embeddings of K into $\mathcal{C}$ and to let s denote the number of pairs of complex embeddings (paired by complex conjugation), so that the total number of embeddings is $r + 2s$. But we have already observed that the number of embeddings is also n (the degree of the number field K), so that $n = r + 2s$.

Example 0.107. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, let γ be the real cube root of 2, as in Example **??**, and let $K = \mathbb{Q}(\alpha)$, which is a number field of degree 3. Any embeddings of K into $\mathcal{C}$ must map γ to one of the roots of $x^3 - 2$, namely $\gamma, \omega\gamma$ or $\omega^2\gamma$, and σ is determined by this choice. For any $a_0 + a_1\gamma + a_2\gamma^2 \in K$, σ must be one of the following three maps. $\sigma_1(a_0 + a_1\gamma + a_2) = a_0 + a_1\gamma + a_2\gamma^2$, $\sigma_2(a_0 + a_1\gamma + a_2) = a_0 + a_1\omega\gamma + a_2\omega^2\gamma^2$, or $\sigma_3(a_0 + a_1\gamma + a_2) = a_0 + a_1\omega^2\gamma + a_2\omega\gamma^2$. We can see that there is one real embedding σ_1, so $r = 1$, and one pair of complex embeddings: σ_2, σ_3, so $s = 1$, consistend with $n = r + 2s = 3$, since indeed the degree n of the number field is 3.

Theorem 0.108. *Let L be a finite field. Then $|L| = p^r$, some prime p and some $r \in \mathbb{N}$.*

Proof Consider $1, 1+1, 1+1+1, \ldots$; since L is finite, there must be repetition at some stage, and we can deduce that there exists $m \in \mathbb{N}$ such that $1 + \ldots + 1$ [m times] $= 0$, and let m be smallest such. However, m must not be composite, say $m = k\ell$ with both factors at least 2, since then $1 + \ldots + 1$ [k times] and $1 + \ldots + 1$ [ℓ times] would each be nonzero, but would multiply to give 0, a contradiction (since L is a field and is therefore an integral domain). So $m = p$, for some prime p, and L contains a subfield K (the subfield generated by the element 1) which is isomorphic to $\mathbb{Z}_p$, so that $|K| = p$. Let $n = [L : K]$, the degree of the

extension (which must be finite, since L is finite) and let $\ell_1, \ldots \ell_n$ be a basis for L over K. Then any $x \in L$ can be written uniquely as $x = k_1\ell_1 + \ldots + k_n\ell_n$, for some $k_1, \ldots, k_n \in K$. Since $|K| = p$, there are p choices for each k_i and so p^n choices for the n-tuple $k_1, \ldots, k_n$; that is to say, there are p^n choices for $x \in L$, so that $|L| = p^n$, as required. □

Comment 0.109. Given p^n for any prime p and any $n \in \mathbb{N}$, it can be shown that the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$ has p^n elements, and so there always exists a field with p^n elements.

The following is the main reference for the lecture course.

Algebraic Number Theory and Fermat's Last Theorem, I. Stewart and D. Tall, Third Edition. This will be frequently cited as "S&T".

Older editions under the name "Algebraic Number Theory" will also suffice.

Other useful but more advanced references:

A Classical Introduction to Modern Number Theory, (Chapter 12) K. Ireland and M. Rosen

Algebraic Number Theory, A. Frohlich and M.J. Taylor

A Course in Computational Algebraic Number Theory, H. Cohen.

The following gives some possible pre-course reading options if you find that you have gaps in your knowledge of any of the pre-requisite material described in Section 0. See also the lecture notes from: Mods Groups, Ring and Fields, Part A Rings, Part A Fields, Part A Number Theory and Part B Galois Theory.

W. Keith Nicholson. *Introduction to Abstract Algebra.* (Second Edition, John Wiley, 1999).

Peter J. Cameron. *Introduction to Algebra.* OUP 1998.

Alan Baker. *A Concise Introduction to the Theory of Numbers.* CUP, 1985.

I.M. Niven, H.S. Zuckerman and H.L. Montgomery. *An Introduction to the Theory of Numbers.* Wiley, 1991.

Chapter 1 (including the exercises) of Steward and Tall, above.

Algebraic Number Theory. Sheet 0.

This sheet is for your own use (it is not intended to be handed in).

(i) Let $q \in \mathbb{Q}$, let r be a non-zero square-free integer (that is: there is no prime p for which $p^2|r$), and let $q^2 r \in \mathbb{Z}$. Show that $q \in \mathbb{Z}$.

(ii) Find the minimal polynomial of $\frac{1+i}{\sqrt{2}}$. What are the other roots of this polynomial?

(iii) Show that $\mathbb{Z}[i]$ is a Euclidean Domain. What are the units in this ring?

(iv) Factorise $6 + 12i$ into irreducibles in $\mathbb{Z}[i]$, and prove that your factors are indeed irreducible.

(v) Let a be a non-zero element of $R := \mathbb{Z}[i]$, and define $A = \{ar : r \in R\}$. Show that R/A is finite. If a is prime show that R/A is an integral domain. Quote an appropriate theorem on finite integral domains, and deduce that A is a maximal ideal of R.

(vi) Let $S = \{m + n\sqrt{-6} : m, n \in \mathbb{Z}\}$, and let I be the ideal of S generated by 2 and $\sqrt{-6}$. Show that S/I has exactly two elements, and deduce that I is a maximal ideal of S.

Reading and Further Practice: Chapter 1 of Stewart and Tall, including the exercises.