OUTLINE OF SOLUTIONS OF SOME OF THE ASSIGNMENTS

1. Week 1

1. (a) Prove that $A := \{a+bi |\ a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{C}$.
   (b) Prove that $B := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$ is a subring of $\mathrm{M}_2(\mathbb{Q})$.
   (c) Prove that A and B are isomorphic.

   Outline of solution. For parts (a) and (b) use the subring criterion. For part (c) prove that

$$f\Big(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \Big) := a + bi$$

   is a ring isomorphism. Notice that the main reason that f is a ring homomorphism is because $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = -I$ and $i^2 = -1$. □

2. An element a of a ring A is called *nilpotent* if $a^n = 0$ for some positive integer n. Suppose A is a unital ring and $a \in A$ is nilpotent. Prove that $1_A + a$ is a unit.

   Solution. Let's recall a useful equation (that you have seen when you learned about geometric series): for every positive integer m (in every unital ring), we have

$$(1-x)(1+x+\cdots+x^m) = 1 - x^{m+1} \quad \text{, and similarly} \quad (1+x+\cdots+x^m)(1-x) = 1 - x^{m+1} \tag{1}$$

   Now suppose A is a unital ring and $y \in A$ is nilpotent and $y^n = 0$ for a positive integer n. Then by (1), we have that

$$(1-y)(1+y+\cdots+y^{n-1}) = 1 - y^n = 1, \quad \text{and similarly} \quad (1+y+\cdots+y^{n-1})(1-y) = 1. \tag{2}$$

   Since A is closed under multiplication and addition, $1+y+\cdots+y^{n-1} \in A$. Therefore (2) implies that $1-y$ is a unit in A. Finally we notice that if a is nilpotent, then $a^n = 0$ for some positive integer n. Thus $(-a)^n = 0$, which means $-a$ is also nilpotent. Hence applying the above result for $y = -a$ we deduce that $1+a$ is a unit in A. □

3. Suppose A and B are unital commutative rings.
   (a) Prove that the identity of $A \times B$ is $(1_A, 1_B)$.
   (b) Prove that the group of units of $A \times B$ is equal to $A^\times \times B^\times$.

   Solution. (a) Notice that for every $(a, b) \in A \times B$, we have

$$(1_A, 1_B) \cdot (a, b) = (1_A \cdot a, 1_B \cdot b) = (a, b), \quad \text{and} \quad (a, b) \cdot (1_A, 1_B) = (a \cdot 1_A, b \cdot 1_B) = (a, b).$$

   This implies that $(1_A, 1_B)$ is an identity of $A \times B$. We have proved that there is a unique identity in a unital ring. Therefore $1_{A\times B} = (1_A, 1_B)$.

   (b) Suppose $(a, b) \in A^\times \times B^\times$. Then there are multiplicative inverses $a^{-1} \in A$ and $b^{-1} \in B$. Therefore

$$(a^{-1}, b^{-1}) \cdot (a, b) = (a^{-1} \cdot a, b^{-1} \cdot b) = (1_A, 1_B) = 1_{A\times B}.$$

   Similarly we have $(a, b) \cdot (a^{-1}, b^{-1}) = 1_{A\times B}$. Hence (a, b) is a unit of $A \times B$.

   Now suppose (a, b) is a unit of $A \times B$. This means there is $(a', b') \in A \times B$ such that

$$(a, b) \cdot (a', b') = (a', b') \cdot (a, b) = 1_{A\times B}.$$

Hence we obtain

$$(a \cdot a', b \cdot b') = (a' \cdot a, b' \cdot b) = (1_A, 1_B),$$

and so $a \cdot a' = a' \cdot a = 1_A$ and $b \cdot b' = b' \cdot b = 1_B$, which implies that $a \in A^\times$ and $b \in B^\times$. □

4. Suppose A is a unital commutative ring and $p1_A = 0$ for a prime p. Let $F : A \to A, F(a) := a^p$. Prove that F is a ring homomorphism.

Solution. We have to show that F preserves addition and multiplication; that means we have to prove that for every $a, a' \in A$ we have

$$F(a + a') = F(a) + F(a') \quad \text{and} \quad F(aa') = F(a)F(a').$$

This means we have to prove $(a + a')^p = a^p + a'^p$ and $(aa')^p = a^p a'^p$. Since A is commutative, we immediately see that

$$(aa')^p = \underbrace{(aa') \cdots (aa')}_{p \text{ times}} = (\underbrace{a \cdots a}_{p \text{ times}})(\underbrace{a' \cdots a'}_{p \text{ times}}) = a^p a'^p.$$

To show that F preserves addition, we notice that since A is commutative we can use the binomial expansion:

$$(a + a')^p = \sum_{i=0}^{p} \binom{p}{i} a^i \cdot a'^{p-i}. \tag{3}$$

Next we notice that $p! = i!(p-i)!\binom{p}{i}$ is a multiple of p and $i!(p-i)!$ is not a multiple of p for integers in the interval $[1, p-1]$. Therefore by Euler's lemma, p divides $\binom{p}{i}$. On the other hand, $p1_A = 0$ implies that for every $b \in A$, we have

$$pb = p(1_A \cdot b) = (p1_A) \cdot b = 0,$$

and so if n is a multiple of p, then for every $b \in A$ we have $nb = 0$.

As $\binom{p}{i}$ is a multiple of p for every integer i in $[1, p-1]$, by the above discussion we deduce that

$$\binom{p}{i} a^i \cdot a'^{p-i} = 0 \tag{4}$$

for every integer i in $[1, p-1]$. By (3) and (4), we obtain

$$(a + a')^p = \sum_{i=0}^{p} \binom{p}{i} a^i \cdot a'^{p-i} = a^p + a'^p.$$

□

5. Describe all the ring homomorphism from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

Solution. Starting with the additive structure of $\mathbb{Z} \times \mathbb{Z}$, we see the every element $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ is an $\mathbb{Z}$-linear combination of $(1, 0)$ and $(0, 1)$. Therefore every ring homomorphism $f : \mathbb{Z} \times \mathbb{Z} \to A$ (for an arbitrary ring A) has the following property:

$$f(m, n) = f(m(1, 0) + n(0, 1)) = mf(1, 0) + nf(0, 1). \tag{5}$$

So f is uniquely determined by its value at $(1, 0)$ and $(0, 1)$. Now that we have understood the additive structure, we focus on multiplication. Suppose $a_1 := f(1, 0)$ and $a_2 := f(0, 1)$. Then we apply f to the following multiplication table:

·	(1,0)	(0,1)
(1,0)	(1,0)	(0,0)
(0,1)	(0,0)	(0,1)

and using the fact that f preserves multiplication we obtain that

$\cdot$	a_1	a_2
a_1	a_1	0
a_2	0	a_2

This means $a_1^2 = a_1$, $a_2^2 = a_2$, and $a_1a_2 = 0$. One can check that these conditions are sufficient to make $f(m,n) = ma_1 + na_2$ a ring homomorphism from $\mathbb{Z}$ to an arbitrary ring A. When $A = \mathbb{Z}$ (in general for every integral domain), we see get the following possibilities for a_i's: either $a_1 = 0$ or $a_1 = 1$, either $a_2 = 0$ or $a_2 = 1$, and either $a_1 = 0$ or $a_2 = 0$. Altogether, we get the following possibilities for a_1 and a_2: either $a_1 = a_2 = 0$, or $a_1 = 1$ and $a_2 = 0$, or $a_1 = 0$ and $a_2 = 1$. Therefore there are three possible ring homomorphisms $f_1 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, f_1(m,n) := 0$, $f_2 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, f_1(m,n) := m$, and $f_3 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, f_1(m,n) := n$. □

2. Week 2

1. (a) Prove that $\mathbb{Q}[\sqrt{3}]$ is a field.
   (b) Prove that $Q(\mathbb{Z}[\sqrt{3}]) \simeq \mathbb{Q}[\sqrt{3}]$ where $\mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} | \, a, b \in \mathbb{Z}\}$ and $Q(\mathbb{Z}[\sqrt{3}])$ is the field of fractions of $\mathbb{Z}[\sqrt{3}]$. (You can use without proof that $\mathbb{Z}[\sqrt{3}]$ is a subring of $\mathbb{C}$.)

Outline of solution. (a) Using the subring criterion, one can see that $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{3}]$ are subrings of $\mathbb{C}$. So to show $\mathbb{Q}[\sqrt{3}]$ is a field, it is enough to show that every non-zero element is a unit. Suppose $a + b\sqrt{3}$ is a non-zero element of $\mathbb{Q}[\sqrt{3}]$. Since $\sqrt{3}$ is not rational, $a - b\sqrt{3}$ is not zero. Hence

$$\frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{(a+b\sqrt{3})(a-b\sqrt{3})} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3}. \tag{6}$$

For $a, b \in \mathbb{Q}$, we have that $\frac{a}{a^2-3b^2}, -\frac{b}{a^2-3b^2} \in \mathbb{Q}$. Therefore (6) implies that $a + b\sqrt{3}$ is a unit in $\mathbb{Q}[\sqrt{3}]$. This shows that $\mathbb{Q}[\sqrt{3}]$ is a field.

(b) We follow the four step strategy explained in the lecture note. We have already proved that $\mathbb{Q}[\sqrt{3}]$ is a field. Let $f : \mathbb{Z}[\sqrt{3}] \to \mathbb{Q}[\sqrt{3}], f(a + b\sqrt{3}) := a + b\sqrt{3}$, and observed that f is an injective ring homomorphism (the 2nd step). Then by the Universal Property of the Field of Fractions,

$$\widetilde{f} : Q(\mathbb{Z}[\sqrt{3}]) \to \mathbb{Q}[\sqrt{3}], \widetilde{f}\Big(\frac{z_1}{z_2}\Big) := f(z_1)f(z_2)^{-1}$$

is an injective ring homomorphism (the 3rd step). In the final step, we should show that $\widetilde{f}$ is surjective. Notice that every element of $\mathbb{Q}[\sqrt{3}]$ is of the form $k^{-1}(m + n\sqrt{3})$ for some integers m, n, k. Then

$$k^{-1}(m + n\sqrt{3}) = \widetilde{f}\Big(\frac{m+n\sqrt{3}}{k}\Big),$$

and so $\widetilde{f}$ is surjective. This shows that $\widetilde{f}$ is an isomorphism. □

2. Suppose p is an odd prime, and let $A := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Z}_p \right\}$.
   (a) Suppose there are $a_0, b_0 \in \mathbb{Z}$ such that $p = a_0^2 + b_0^2$. Prove that $A \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.
   (b) Suppose there is no $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod{p}$. Prove that A is a field.

Outline of solution. (a) The key point is to notice that $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ should be sent to an element that is a zero of $x^2 = -1$ in the codomain. So we start by finding zeros of $x^2 = -1$ in $\mathbb{Z}_p$. Since $p = a_0^2 + b_0^2$, $0 \equiv a_0^2 + b_0^2 \pmod{p}$. If $b_0 \not\equiv 0 \pmod{p}$, then b_0 is a unit in $\mathbb{Z}_p$. Hence we get

$$(a_0 b_0^{-1})^2 = -1 \text{ in } \mathbb{Z}_p.$$

Next we argue that $b_0 \neq 0$ in $\mathbb{Z}_p$. If not, then b_0 is a multiple of p. On the other hand, $p = a_0^2 + b_0^2$ implies that $|b_0| \sqrt{p}$. The only multiple of b_0 which is in the interval $[-\sqrt{p}, \sqrt{p}]$ is 0. Therefore $b_0 = 0$,

and so $p = a_0^2$ which is a contradiction as p is prime. Altogether we deduce that there is $e \in \mathbb{Z}_p$ such that $e^2 = -1$. Let

$$f : A \to \mathbb{Z}_p \times \mathbb{Z}_p,\ f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = (a + eb, a - eb).$$

One can easily check that f is a ring homomorphism. Since A and $\mathbb{Z}_p \times \mathbb{Z}_p$ have p^2 elements, it is enough to show that f is injective in order to deduce that f is a bijection. To show that f is injective, we have to show that the kernel of f is trivial. Suppose $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \ker f$. Then $a + eb = a - eb = 0$. Adding these equations, we obtain that $2a = 0$. Since p is odd, we deduce that $a = 0$. Having $a = 0$ and $a + eb = 0$, we get that $b = 0$. Therefore the kernel is trivial, which finishes the proof.

(b) One can check that A is commutative. So to show that A is a field, it is enough to prove that every non-zero element of A is a unit. We know that

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix}\begin{pmatrix} t & -y \\ -z & x \end{pmatrix} = \begin{pmatrix} xt - yz & 0 \\ 0 & xt - yz \end{pmatrix},$$

whenever the entries are in a commutative ring. Hence for $a, b \in \mathbb{Z}_p$ we have

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2 + b^2 & 0 \\ 0 & a^2 + b^2 \end{pmatrix}. \tag{7}$$

If $a^2 + b^2 \neq 0$ in $\mathbb{Z}_p$, then it has a multiplicative inverse in $\mathbb{Z}_p$ and by (7) we obtain that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = (a^2 + b^2)^{-1}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in A.$$

So it only remains to show that $a^2 + b^2 \neq 0$ if either $a \neq 0$ or $b \neq 0$. To the contrary, let's assume that $a^2 + b^2 = 0$ and without loss of generality let's assume that $a \neq 0$. Then a is a unit in $\mathbb{Z}_p$, and so $b^2 = -a^2$ implies that

$$(a^{-1}b)^2 = -1,$$

which contradicts the assumption that $x^2 = -1$ does not have a zero in $\mathbb{Z}_p$. □

3. Find the characteristic of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ where m_i's are positive integers.

Outline of solution. As it is proved in the lecture, if the additive order of 1_A is finite, then the characteristic of A coincides with the additive order of 1_A. The identity of $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ is $([1]_{m_1}, \cdots, [1]_{m_k})$. The following help us to find the additive order of this element:

$$\begin{aligned} n([1]_{m_1}, \cdots, [1]_{m_k}) =& ([0]_{m_1}, \cdots, [0]_{m_k}) \\ \Leftrightarrow& \forall i, n[1]_{m_i} = [0]_{m_i} \\ \Leftrightarrow& \forall i, m_i | n \\ \Leftrightarrow& \operatorname{lcm}(m_1, \ldots, m_k) | n. \end{aligned}$$

Hence the smallest positive such n is $\operatorname{lcm}(m_1, \ldots, m_k)$. □

4. Suppose p is prime and a is a non-zero element of $\mathbb{Z}_p$. Prove that $x^p - x + a$ has no zero in $\mathbb{Z}_p$.

Solution. By the Fermat's little theorem, for every $b \in \mathbb{Z}_p$ we have $b^p = b$. This means the value of $x^p - x + a$ at $x = b$ is $b^p - b + a = a \neq 0$. Hence $x^p - x + a$ has no zero in $\mathbb{Z}_p$.

□

5. (a) Show that $x^2 - 5$ does not have a zero in $\mathbb{Q}[\sqrt{2}]$.
(b) Prove that $\mathbb{Q}[\sqrt{2}]$ is not isomorphic to $\mathbb{Q}[\sqrt{5}]$.

Outline of solution. Suppose to the contrary that there are $a, b \in \mathbb{Q}$ such that $(a+b\sqrt{2})^2 = 5$. Then we have

$$(a^2 + 2b^2) + (2ab)\sqrt{2} = 5. \tag{8}$$

Since $\sqrt{2}$ is irrational, from (8) we deduce that

$$a^2 + 2b^2 = 5 \text{ and } 2ab = 0. \tag{9}$$

This implies that either $a = 0$ or $b = 0$. If $a = 0$, then by (9) we have that $2b^2 = 5$ which is a contradiction as $\sqrt{5/2}$ is irrational. Similarly if $b = 0$, then by (9) we have that $a^2 = 5$ which is a contradiction as $\sqrt{5}$ is irrational.

(b) Suppose to the contrary that there is a ring isomorphism $f : \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}[\sqrt{2}]$. Then $f(1) \neq 0$ (it is injective) and $f(1)^2 = f(1)$. Hence $f(1) = 1$. Hence for every integer n we have $f(n) = n$. Now notice that $f(\sqrt{5})^2 = f(5) = 5$. This contradicts part (a) as $f(\sqrt{5}) \in \mathbb{Q}[\sqrt{2}]$ would be a zero of $x^2 - 5$. □

3. Week 3

1. Find all the primes p such that $x + 2$ is a factor of

$$x^6 - x^4 + x^3 - x + 1$$

in $\mathbb{Z}_p[x]$.

Solution. By the factor theorem we know that $x + 2$ is a factor of $f(x) := x^6 - x^4 + x^3 - x + 1$ in $\mathbb{Z}_p$ if and only if $f(-2) = 0$ in $\mathbb{Z}_p$. This later happens if and only if p divides

$$f(-2) = (-2)^6 - (-2)^4 + (-2)^3 - (-2) + 1 = 64 - 16 - 8 + 2 + 1 = 43.$$

Since 43 is prime, we deduce that the only possible p is 43. □

2. Find a zero of $x^3 - 2x + 1$ in $\mathbb{Z}_5$ and express is as a product of a degree 1 and a degree 2 polynomial.

Solution. One can see that 1 is a zero of this polynomial. By the long division algorithm, we divide $x^3 - 2x + 1$ by $x - 1$, and get that

$$x^3 - 2x + 1 = (x - 1)(x^2 + x - 1).$$

□

3. Recall that in earlier using the binomial expansion we have proved that $(x - 1)^p = x^p - 1$ in $\mathbb{Z}_p[x]$ when p is an odd prime. Use this result to show that

$$\binom{p-1}{i} \equiv (-1)^i \pmod{p}$$

for an odd prime p and an integer i in the range $[0, p - 1]$.

Proof. We have that

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + 1). \tag{10}$$

By (10) and $(x - 1)^p = x^p - 1$, we have

$$(x - 1)^p = (x - 1)(x^{p-1} + x^{p-2} + \cdots + 1). \tag{11}$$

Since $\mathbb{Z}_p$ is an integral domain, so is $\mathbb{Z}_p[x]$. Hence the cancellation law holds in $\mathbb{Z}_p[x]$. Therefore by (11), we have

$$(x - 1)^{p-1} = x^{p-1} + \cdots + 1. \tag{12}$$

This means the coefficients of x^i in the left hand side and in the right hand side are equal:

$$(-1)^{p-1-i}\binom{p-1}{i} \equiv 1 \pmod{p}.$$

Since p is odd, $(-1)^{p-1} = 1$ and the claim follows. □

4. Let $\omega := \frac{-1+\sqrt{-3}}{2}$, and let $\mathbb{Z}[\omega]$ be the image of the evaluation map $\phi_\omega : \mathbb{Z}[x] \to \mathbb{C}$.
   (a) Prove that $\mathbb{Z}[\omega] = \{a + b\omega |\ a, b \in \mathbb{Z}\}$.
   (b) Show that the field of fraction of $\mathbb{Z}[\omega]$ is $\{a + b\omega |\ a, b \in \mathbb{Q}\}$.
   (Notice that $\omega^2 + \omega + 1 = 0$. Deduce that $\omega + \overline{\omega} = -1$ and $\omega\overline{\omega} = 1$ where $\overline{\omega}$ is the complex conjugate of ω. Using these equations, deduce that $(a + b\omega)(a + b\overline{\omega}) = a^2 - ab + b^2$.)

Outline of solution. (a) We know that $\mathbb{Z}[\omega]$ is the smallest ring which contains $\mathbb{Z}$ and ω. Also notice that every subring of $\mathbb{C}$ that contains $\mathbb{Z}$ and ω, also contains $A := \{a + b\omega \mid a, b \in \mathbb{Z}\}$ as a subset. So if we show that A is a ring, we deduce that $A = \mathbb{Z}[\omega]$. You can use the subring criterion to show that A is a subring.

(b) Step 1. We show that $F := \{a + b\omega \mid a, b \in \mathbb{Q}\}$ is a field. First using the subring criterion, one can show that this is a subring of $\mathbb{C}$. Next we show that every non-zero element of F is a unit:

$$\frac{1}{a+b\omega} = \frac{a+b\overline{\omega}}{a^2-ab+b^2} = \frac{a-b(\omega+1)}{a^2-ab+b^2} = \frac{a-b}{a^2-ab+b^2} - \frac{b}{a^2-ab+b^2}\omega \in F.$$

Step 2. Let $f : \mathbb{Z}[\omega] \to \mathbb{Q}[\omega], f(z) := z$ be the natural embedding.

Step 3. By the universal property of field of fractions, there is an embedding $\widetilde{f} : Q(\mathbb{Z}[\omega]) \to \mathbb{Q}[\omega]$ such that

$$\widetilde{f}\Big(\frac{z_1}{z_2}\Big) = f(z_1)f(z_2)^{-1} = z_1 z_2^{-1}.$$

Step 4. We show that $\widetilde{f}$ is surjective. Every element of $\mathbb{Q}[\omega]$ is of the form $\frac{r+s\omega}{t}$ for some integers r, s, and t. Then

$$\frac{r+s\omega}{t} = \widetilde{f}\Big(\frac{r+s\omega}{t}\Big).$$

□

5. In the setting of problem 4, Let $N : \mathbb{Z}[\omega] \to \mathbb{Z}^{\geq 0}, N(z) := |z|^2$.
   (a) Show that we can view N as a norm function of $\mathbb{Z}[\omega]$, and deduce that $\mathbb{Z}[\omega]$ is a Euclidean domain. (*Hint.* Use the tiling given in Figure 1 to prove the division property of Euclidean domains)
   (b) Prove that $\mathbb{Z}[\omega]$ is a PID.

Proof. (a) Notice that $N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 - ab + b^2 \in \mathbb{Z}^{\geq 0}$ for every $a, b \in \mathbb{Z}$. We also have that $N(z) = 0$ if and only if $|z| = 0$. Hence $N(z) = 0$ if and only if $z = 0$.

For every $z_1 \in \mathbb{Z}[\omega]$ and $z_2 \in \mathbb{Z}[\omega] \setminus \{0\}$, consider the complex number $\frac{z_1}{z_2}$. This complex number belongs to one the hexagon in the tiling. Let $q \in \mathbb{Z}[\omega]$ be the center of this hexagon. Then $\frac{z_1}{z_2} - q$ belongs to the hexagon in the tiling whose center is 0. Hence $\left|\frac{z_1}{z_2} - q\right| < 1$. Let

$$r := z_2\Big(\frac{z_1}{z_2} - q\Big) = z_1 - qz_2.$$

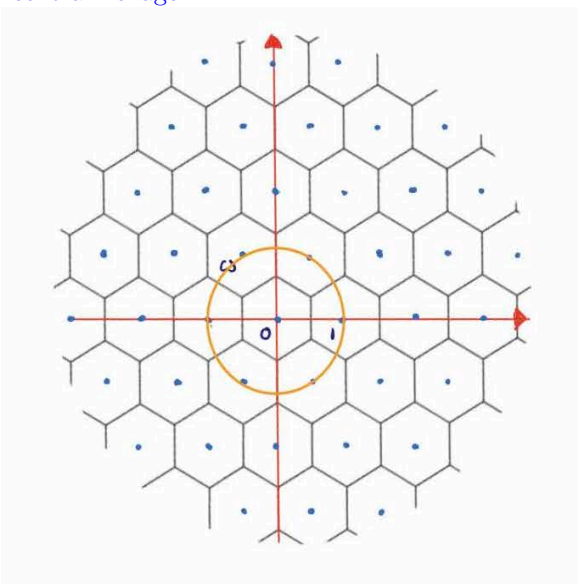
Then $|r| < |z_2|$. As z_1, z_2, and q are in $\mathbb{Z}[\omega]$, we have that $r \in \mathbb{Z}[\omega]$. Overall we found $r, q \in \mathbb{Z}[\omega]$ such that

$$z_1 = qz_2 + r \quad \text{and} \quad N(r) < N(z_2).$$

This means that $\mathbb{Z}[\omega]$ is a Euclidean domain.

(b) We know that every Euclidean domain is a PID. □

FIGURE 1. This tiling shows that every complex point after a shift by an element of $\mathbb{Z}[\omega]$ can be moved to the central hexagon.



4. WEEK 4

1. Prove that $|\mathbb{Z}_m[x]/\langle\sum_{i=0}^n a_i x^i\rangle| = m^n$ if $a_n \in \mathbb{Z}_m^\times$.

For every $f(x) \in \mathbb{Z}_m[x]$, by the long division there are unique $q(x), r(x) \in \mathbb{Z}_m[x]$ such that

$$f(x) = q(x)(\sum_{i=0}^n a_i x^i) + r(x) \quad \text{and} \quad \deg r < n.$$

Notice that since the leading coefficient of $\sum_{i=0}^n a_i x^i$ is a unit, we can apply the long division. So every element $f(x) + \langle\sum_{i=0}^n a_i x^i\rangle$ can be uniquely written as $r(x) + \langle\sum_{i=0}^n a_i x^i\rangle$ for some polynomial $r(x) \in \mathbb{Z}_m$ of degree less than n. Notice that $r(x) = \sum_{i=0}^{n-1} b_i x^i$ for some $b_i \in \mathbb{Z}_m$. For each i, there are m choices for b_i. Hence there are m^n polynomials of degree less than n in $\mathbb{Z}_m[x]$. This implies that

$$\left|\mathbb{Z}_m[x]/\left\langle \sum_{i=0}^n a_i x^i \right\rangle\right| = m^n.$$

2. Let

$$c_3 : \mathbb{Z}_6[x] \to \mathbb{Z}_3[x],\ c_3\Big(\sum_{i=0}^n [a_i]_6 x^i\Big) = \sum_{i=0}^n [a_i]_3 x^i,$$
$$\phi_{-1} : \mathbb{Z}_3[x] \to \mathbb{Z}_3,\ \phi_{-1}(f(x)) := f(-1), \quad \text{and}$$
$$\psi : \mathbb{Z}_6[x] \to \mathbb{Z}_3,\ \psi(f(x)) := \phi_{-1}(c_3(f(x))).$$

You have already seen that c_3 and ϕ_{-1} are surjective ring homomorphisms, and so you can deduce that ψ is also a surjective ring homomorphism.

(a) Use the factor theorem, to show that $\ker \phi_{-1} = \langle x + [1]_3\rangle$.

We have that $f(x) \in \ker \phi_{-1}$ if and only if -1 is a zero of f. By the factor theorem, -1 is a zero of f if and only if $f(x)$ is a multiple of $x + [-1]_3$. The claim follows.

(b) Prove that $\ker\psi = \langle x+1, 3\rangle$. (Notice that here $1 = [1]_6$ and $3 = [3]_6$.)

Since $\psi = \phi_{-1} \circ c_3$, by part (a) we have that $f \in \ker\psi$ if and only if $c_3(f)$ is a multiple of $x + [1]_3$. Since c_3 is surjective, we have that $f \in \ker\psi$ if and only if $c_3(f) = c_3(x+1)c_3(g)$ for some $g \in \mathbb{Z}_6[x]$. Notice that $c_3(f) = c_3((x+1)g)$ if and only if $f(x) = (x+1)g(x) + 3h(x)$ for some $h \in \mathbb{Z}_6[x]$. Altogether we have that $f(x) \in \ker\psi$ if and only if $f(x) \in \langle x+1, 3\rangle$. This proves the claim.

(c) Prove that $\ker\psi = \langle 2x-1\rangle$.

Since $2x - 1 = 2(x+1) - 3 \in \langle x+1, 3\rangle$, we have that $\langle 2x-1\rangle \subseteq \langle x+1, 3\rangle$. On the other hand, $3(2x-1) = 3 \in \langle 2x-1\rangle$, which implies that $x + 1 = 3x - (2x-1) \in \langle 2x-1\rangle$. Therefore $\langle 3, x+1\rangle \subseteq \langle 2x-1\rangle$. This completes the proof.

(d) Prove that $\mathbb{Z}_6[x]/\langle 2x-1\rangle \simeq \mathbb{Z}_3$.

Since c_3 and ϕ_{-1} are surjective, so is ψ. Hence by part (c) and the first isomorphism theorem, we obtain part (d).

(e) Explain why $|\mathbb{Z}_6[x]/\langle 2x-1\rangle| = 3 \neq 6^1$ does not contradict the first problem.

It is not a contradiction as the leading coefficient 2 of $2x - 1$ is not a unit in $\mathbb{Z}_6$, but this condition is needed in the first problem.

3. Find the minimal polynomial $m_{\sqrt[3]{5}}(x)$ of $\sqrt[3]{5}$ over $\mathbb{Q}$.

We know that $\sqrt[3]{5}$ is a zero of $x^3 - 5$. We use the degree 2 or 3 irreducibility criterion, it is enough to show that $x^3 - 5$ does not have a rational zero. This is the case as $\sqrt[3]{5}$ is not rational. So $\sqrt[3]{5}$ is a zero of the monic irreducible polynomial $x^3 - 5 \in \mathbb{Q}[x]$. Hence $m_{\sqrt[3]{5},\mathbb{Q}}(x) = x^3 - 5$.

4. Suppose $p(x) \in \mathbb{Q}[x]$ is a degree 3 monic polynomial with no rational zeros. Let $\alpha \in \mathbb{C}$ be a zero of $p(x)$. Prove that the minimal polynomial of α over $\mathbb{Q}$ is $p(x)$.

By the degree 2 or 3 irreducibility criterion, $p(x)$ is irreducible. Since α is a zero of p and p is monic irreducible in $\mathbb{Q}[x]$, $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

5. Suppose p is a prime more than 3 and $p = a_0^2 - a_0b_0 + b_0^2$ for some integers a_0 and b_0.

(a) Prove that $x^2 + x + 1$ has a zero $[e]_p$ in $\mathbb{Z}_p$ such that $p | a_0 + b_0 e$.

Considering $p = a_0^2 - a_0b_0 + b_0^2$ modulo p, we have $0 = a_0^2 - a_0b_0 + b_0^2$ in $\mathbb{Z}_p$. If $b_0 \neq 0$ in $\mathbb{Z}_p$, then it is a unit in $\mathbb{Z}_p$. In this case, we have

$$(b_0^{-1}a_0)^2 - (b_0^{-1}a_0) + 1 = 0,$$

which implies that $-b_0^{-1}a_0$ is a zero of $x^2 + x + 1$ in $\mathbb{Z}_p$. If $b_0 = 0$ in $\mathbb{Z}_p$, then we deduce that $a_0^2 = 0$ in $\mathbb{Z}_p$. In this case, both a_0 and b_0 are multiples p. Therefore p^2 divides $a_0^2 - a_0b_0 + b_0^2 = p$, which is a contradiction. Hence $e := -b_0^{-1}a_0$ in $\mathbb{Z}_p$ is a zero of $x^2 + x + 1$. Notice that $a_0 + b_0 e = 0$ in $\mathbb{Z}_p$.

(b) Let $\omega := \frac{-1+\sqrt{-3}}{2}$, and $f : \mathbb{Z}[\omega] \to \mathbb{Z}_p$, $f(a + b\omega) := [a + be]_p$, where e is given in part (a). Show that f is a surjective ring homomorphism and $a_0 + b_0\omega \in \ker f$.

Check that f is a ring homomorphism. Since $f(a) = [a]_p$ for every $a \in \mathbb{Z}$, f is surjective. We have

$$f(a_0 + b_0\omega) = [a_0 + b_0 e]_p = 0;$$

and so $a_0 + b_0\omega \in \ker f$.

(c) Use the fact that $\mathbb{Z}[\omega]$ is a PID, and prove that $\ker f = \langle a_0 + b_0\omega\rangle$.

Since $\mathbb{Z}[\omega]$ is a PID, $\ker f$ is a principal ideal. Suppose that $\ker f$ is generated by z. Since $a_0 + b_0\omega \in \ker f$, there is $z' \in \mathbb{Z}[\omega]$ such that $a_0 + b_0\omega = zz'$. Recall that $N : \mathbb{Z}[\omega] \to \mathbb{Z}^{\geq 0}, N(x) := |x|^2$ is a well-defined multiplicative function. Hence

$$p = N(a_0 + b_0\omega) = N(z)N(z').$$

As p is prime, either $N(z) = 1$ or $N(z') = 1$. Notice that $\overline{\omega} \in \mathbb{Z}[\omega]$; and so for every $x \in \mathbb{Z}[\omega]$ we have that $\overline{x} \in \mathbb{Z}[\omega]$. This implies that if $N(x) = 1$, then x is a unit in $\mathbb{Z}[\omega]$. Since f is surjective, its kernel is a proper ideal. Hence z cannot be a unit. Therefore z' is a unit, which implies that

$$\ker f = \langle z\rangle = \langle z'z\rangle = \langle a_0 + b_0\omega\rangle.$$

(d) Prove that

$$\mathbb{Z}[\omega]/\langle a_0 + b_0\omega\rangle \simeq \mathbb{Z}_p,$$

This immediately follows from the previous steps and the first isomorphism theorem.

5. Week 5

1. Let $I := \langle x, y\rangle \lhd \mathbb{C}[x, y]$.

(a) Prove that I is a maximal ideal of $\mathbb{C}[x, y]$.

Let $\phi_{(0,0)} : \mathbb{C}[x, y] \to \mathbb{C}, \phi_{(0,0)}(f(x, y)) := f(0, 0)$ be the map of evaluation at $(0, 0)$. Then $\phi_{(0,0)}$ is a ring homomorphism. For every $c \in \mathbb{C}$, we have that $\phi_{(0,0)}(c) = c$, where c is viewed as a constant polynomial. Hence $\phi_{(0,0)}$ is surjective. Notice that $\phi_{(0,0)}(x) = \phi_{(0,0)}(y) = 0$. Hence $\langle x, y\rangle \subseteq \ker \phi_{(0,0)}$. We also observe that $x^i y^j \in \langle x, y\rangle$ if either $i \neq 0$ or $j \neq 0$. Hence every polynomial f can be written as

$$f(0, 0) + xp(x, y) + yq(x, y) \tag{13}$$

for some $p, q \in \mathbb{C}[x]$. Because of (13), we have that if $f \in \ker \phi_{(0,0)}$, then $f \in \langle x, y\rangle$. Altogether we deduce that $\ker \phi_{(0,0)} = \langle x, y\rangle$. Therefore by the first isomorphism theorem, we have that

$$\mathbb{C}[x, y]/\langle x, y\rangle \simeq \mathbb{C},$$

Hence $\mathbb{C}[x, y]/\langle x, y\rangle$ is a field, which implies that $\langle x, y\rangle$ is a maximal ideal.

(b) Prove that I is not principal.

Suppose to the contrary that I is a principal ideal and it is generated by the polynomial $f(x, y)$. Then there are polynomials p, q such that $x = f(x, y)p(x, y)$ and $y = f(x, y)q(x, y)$. Viewing these polynomials as elements of $(\mathbb{C}[x])[y]$, we can talk about their degree in terms of y. Since $\mathbb{C}[x]$ is an integral domain, so is $\mathbb{C}[x, y]$. Hence the degree of product is the summation of degrees. Therefore

$$\underbrace{\deg_y x}_{0} = \deg_y f + \deg_y p \quad \text{and} \quad \underbrace{\deg_x y}_{0} = \deg_x f + \deg_x q. \tag{14}$$

By (14) we obtain that $\deg_y f = \deg_x f = 0$. This means $f(x, y) = c$ is a constant polynomial. Therefore $\langle f\rangle$ is either $\{0\}$ or $\mathbb{C}[x, y]$. But neither of these options are possible as $\langle f\rangle = \langle x, y\rangle$ is a maximal ideal by the first part.

2. Let $D = \mathbb{Z}[\sqrt{-21}]$ and $N(z) := |z|^2$.

(a) Prove that $z \in D^\times$ if and only if $N(z) = 1$. Then deduce that $D^\times = \{-1, 1\}$.

($\Rightarrow$) We have that $N(zz') = |zz'|^2 = (|z||z'|)^2 = |z|^2|z'|^2 = N(z)N(z')$. Therefore

$$z \in D^\times \Rightarrow \exists z' \in D, zz' = 1 \Rightarrow \exists z' \in D, N(zz') = N(1) = 1 \Rightarrow N(z)N(z') = 1.$$

Since $N(z)$ and $N(z')$ are non-negative integers, $N(z)N(z') = 1$ implies that $N(z) = 1$.
($\Leftarrow$) If $N(z) = 1$, then $z\overline{z} = 1$ where $\overline{z}$ is the complex conjugate of z. Notice that for $z \in D$, we have that $\overline{z} \in D$. Hence $z\overline{z} = 1$ implies that $z \in D^\times$.
Suppose $z = a + b\sqrt{-21}$. We have proved that $z \in D^\times$ if and only if $N(z) = 1$. Hence we have to find all the integer solutions of $a^2 + 21b^2 = 1$. Notice if b is a non-zero integer, then $a^2 + 21b^2 \geq 21$. Therefore if a, b are integers and $a^2 + 21b^2 = 1$, then $b = 0$. This in turn implies that $a^2 = 1$. Thus the only integer solutions of $a^2 + 21b^2 = 1$ are $a = \pm 1$ and $b = 0$. Therefore $D^\times = \{\pm 1\}$.

(b) Prove that $\sqrt{-21}$ is irreducible in D.

Notice $N(\sqrt{-21}) = 21$. Hence by the first part, we have that $\sqrt{-21}$ is not a unit (and clearly it is not zero). So to show it is irreducible it is enough to prove that $\sqrt{-21} = z_1 z_2$ for some $z_1, z_2 \in D$ implies that either z_1 or z_2 is a unit. Taking norm of both sides, we obtain that $21 = N(z_1)N(z_2)$. Therefore $N(z_i)$'s are non-negative divisors of 21. If neither z_1 nor z_2 is a unit, then by part (a) we deduce that either $N(z_1) = 3$ or $N(z_2) = 3$. Hence to show that $\sqrt{-21}$ is irreducible, it is sufficient to argue why there is no $z \in D$ such that $N(z) = 3$. This is equivalent to showing that the equation $a^2 + 21b^2 = 3$ does not have an integer solution. We again notice if b is a non-zero integer, then $a^2 + 21b^2 \geq 21$. Hence for integer numbers a and b, $a^2 + 21b^2 = 3$ implies that $b = 0$. In turn, we deduce that $a^2 = 3$, which does not have an integer solution.

(c) Show that $D/\langle\sqrt{-21}\rangle$ is not an integral domain.

Notice that $3 \times 7 = 21 = -\sqrt{-21}\sqrt{-21} \in \langle\sqrt{-21}\rangle$. Hence $(3 + \langle\sqrt{-21}\rangle)(7 + \langle\sqrt{-21}\rangle) = 0$ in $D/\langle\sqrt{-21}\rangle$. If this quotient ring is an integral domain, then either $3 + \langle\sqrt{-21}\rangle = 0$ or $7 + \langle\sqrt{-21}\rangle = 0$. This means either there is $z \in D$ such that $3 = z\sqrt{-21}$ or there is $z \in D$ such that $7 = z\sqrt{21}$. Taking the norm of all these elements, we deduce that either $9 = 21N(z)$ or $49 = 21N(z)$ for some $z \in D$. This is a contradiction as $21 \nmid 9$ and $21 \nmid 49$.

(d) Deduce that D is not a PID.

Suppose to the contrary that D is a PID. Then the ideal generated by an irreducible element is maximal. Hence the ideal generated by $\sqrt{-21}$ should be a maximal ideal. The quotient ring by a maximal ideal is a field. Therefore $D/\langle\sqrt{-21}\rangle$ should be a field; in particular, it has to be an integral domain. This, however, contradicts part (c).

3. Suppose p is prime and E is a field extension of $\mathbb{Z}_p$. Suppose there is $\alpha \in E$ which is a zero of $x^p - x + 1$.

(a) Prove that $x^p - x + 1 = (x - \alpha) \cdots (x - \alpha - p + 1)$.

Solution 1. Notice that $1_{\mathbb{Z}_p}^2 = 1_{\mathbb{Z}_p} = 1_{\mathbb{Z}_p} 1_E$, and so $1_{\mathbb{Z}_p} = 1_E$. Therefore the characteristic of E is equal to the characteristic of $\mathbb{Z}_p$, and it is p. Hence for every $a, b \in E$, we have that $(a + b)^p = a^p + b^p$. This implies that for every $i \in \mathbb{Z}_p$ we have

$$(\alpha + i)^p - (\alpha + i) + 1 = \alpha^p + i^p - \alpha - i + 1 = (\alpha^p - \alpha + 1) + (i^p - i) = 0$$

where the last equality holds because of Fermat's little theorem and the assumption that $\alpha \in E$ is a zero of $x^p - x + 1$. Therefore $\alpha, \alpha + 1, \ldots, \alpha + (p - 1)$ are p distinct zeros of $x^p - x + 1$.

By the generalized factor theorem (notice that since E is an integral domain, we are allowed to use the generalized factor theorem), we have that

$$x^p - x + 1 = (x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1)f(x) \tag{15}$$

for some $f(x) \in E[x]$. Comparing the degrees of both sides, we deduce that $\deg f = 0$, and so $f(x) = c$ is a non-zero constant. Comparing the leading coefficients of (15), we obtain that $f(x) = c = 1$. Hence

$$x^p - x + 1 = (x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1).$$

Solution 2. We have proved that $x^p - x = x(x-1)\cdots(x-p+1)$ in $\mathbb{Z}_p[x] \subseteq E[x]$. Substituting $x-\alpha$ for x, we obtain

$$(x-\alpha)^p - (x-\alpha) = (x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1).$$

Since the characteristic of E is p, we have $(x-\alpha)^p = x^p - \alpha^p$, and so

$$(x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1) = x^p - x - (\alpha^p - \alpha). \tag{16}$$

Since α is a zero of $x^p - x + 1$, we have that $\alpha^p - \alpha = -1$. Hence by (16), we obtain

$$x^p - x + 1 = (x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1).$$

(b) Prove that $m_{\alpha,\mathbb{Z}_p}(x) = x^p - x + 1$. (Hint. Use part (a) and $m_{\alpha,\mathbb{Z}_p}(x) | x^p - x + 1$.)

Since α is a zero of $x^p - x + 1 \in \mathbb{Z}_p[x]$, the minimal polynomial $m_{\alpha,\mathbb{Z}_p}(x)$ of α over $\mathbb{Z}_p$ divides $x^p - x + 1$. This means that there is $p(x) \in \mathbb{Z}_p[x]$ such that

$$m_{\alpha,\mathbb{Z}_p}(x)p(x) = (x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1). \tag{17}$$

This means for every $i \in \mathbb{Z}_p$, we have that either $m_{\alpha,\mathbb{Z}_p}(\alpha+i) = 0$ or $p(\alpha+i) = 0$. Next we discuss why $\alpha+i$ cannot be a zero of both of the factors $m_{\alpha,\mathbb{Z}_p}(x)$ and $p(x)$. Notice that for a given i, if $\alpha+i$ is a zero of $m_{\alpha,\mathbb{Z}_p}(x)$, then by the factor theorem there $m_{\alpha,\mathbb{Z}_p}(x) = (x-\alpha-i)f(x)$ for some $f(x) \in \mathbb{Z}_p[x]$. This implies that

$$f(\alpha+i)p(\alpha+i) = \prod_{j\neq i}((\alpha+i)-(\alpha+j)) \neq 0.$$

This means we get a partition of the set of zeros $\{\alpha+i \mid i \in \mathbb{Z}_p\}$ into two sets. The first set consists of elements that are zeros of $m_{\alpha,\mathbb{Z}_p}(x)$ and the second set consists of zeros of $p(x)$. Now using the generalized factor theorem and the fact that $m_{\alpha,\mathbb{Z}_p}(x)$ is a monic polynomial, after comparing the degrees we deduce that

$$m_{\alpha,\mathbb{Z}_p}(x) = (x-\alpha-i_1)\cdots(x-\alpha-i_k) \tag{18}$$

for some subset $\{i_1,\ldots,i_k\}$.

This part of the argument gets significantly simplified using the uniqueness of factorization and the fact that degree one factors are irreducible: since $m_{\alpha,\mathbb{Z}_p}(x)$ is a monic divisor of

$$(x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1),$$

it is a product of a subset of these irreducible factors. This immediately takes us to (18).[1] From (18), we have that the coefficient of x^{k-1} in $m_{\alpha,\mathbb{Z}_p}(x)$ is $-(k\alpha + i_1 + \cdots + i_k)$. As all the coefficients of $m_{\alpha,\mathbb{Z}_p}(x)$ are in $\mathbb{Z}_p$ and i_j's are in $\mathbb{Z}_p$, we deduce that $k\alpha \in \mathbb{Z}_p$. If $k \neq p$, then k is a positive integer less than p. Hence it is a unit in $\mathbb{Z}_p$. Therefore $k\alpha \in \mathbb{Z}_p$ implies that $\alpha \in \mathbb{Z}_p$. In this case, by Fermat's little theorem, we have that $\alpha^p = \alpha$. This shows that $\alpha^p - \alpha + 1 = 1 \neq 0$, which means α cannot be a zero of $x^p - x + 1$, and we reach to a contradiction. Altogether we obtain that $k = p$, which means that $\deg m_{\alpha,\mathbb{Z}_p}(x) = p$. Therefore $m_{\alpha,\mathbb{Z}_p}(x) = x^p - x + 1$.

[1] For the purposes of this HW assignment it is was OK to jus make this deduction with no further details.

(c) Deduce that $x^p - x + 1$ is irreducible in $\mathbb{Z}_p[x]$.

The minimal polynomial of every algebraic element over a field is irreducible. Since $x^p - x + 1 = m_{\alpha,\mathbb{Z}_p}(x)$, we deduce that $x^p - x + 1$ is irreducible in $\mathbb{Z}_p[x]$.

4. Prove that $f(x) := x^5 - 15x^3 + 10x^2 - 21x + 2021$ is irreducible in $\mathbb{Q}[x]$. (Hint: Use Problem 3)

Notice that $f(x)$ modulo 5 is $x^5 - x + 1$ which is irreducible by problem 3. Moreover $f(x)$ is a monic polynomial, and so by the mod-p criterion, we have that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

6. Week 6

(Thanks to Alex Mathers for providing these solutions.)

1. Suppose A is a Noetherian unital commutative ring and I is an ideal of A. Prove that A/I is Noetherian.

We give two solutions: for both solutions we recall that every ideal of $\bar{J} \triangleleft A/I$ can be written in the form $\bar{J} = J/I$ for an ideal $J \triangleleft A$ containing I.

Solution 1. Consider an ascending chain of ideals $\bar{J}_1 \subseteq \bar{J}_2 \subseteq \cdots$ of A/I. Per our remark, each ideal $\bar{J}_i$ can be written in the form $\bar{J}_i = J_i/I$ for an ideal $J_i \triangleleft A$ containing I. Then we claim $J_i/I \subseteq J_{i+1}/I$ implies $J_i \subseteq J_{i+1}$: if $a \in J_i$ then $a + I \in J_i/I \subseteq J_{i+1}/I$, so $a + I = x + I$ for some $x \in J_{i+1}$, and from this we see there is some $y \in I \subseteq J_{i+1}$ such that $a = x + y \in J_{i+1}$.

With this in mind we see we have an ascending chain $J_1 \subseteq J_2 \subseteq \cdots$ of ideals of A, and applying the Noetherian hypothesis we see there is some n_0 such that $J_{n_0} = J_{n_0+1} = \cdots$. From this we conclude $\bar{J}_{n_0} = \bar{J}_{n_0+1} = \cdots$, which proves A/I is Noetherian.

Solution 2. Recall a unital commutative ring is Noetherian if and only if every ideal is finitely generated. Consider an ideal $\bar{J} \triangleleft A/I$, which per our remark above has the form $\bar{J} = J/I$ for an ideal $J \triangleleft A$ containing I. Because A is Noetherian, the ideal J is finitely generated, say $J = \langle x_1, \ldots, x_n \rangle$. Then we claim $J/I = \langle x_1 + I, \ldots, x_n + I \rangle$. The inclusion $\langle x_1 + I, \ldots, x_n + I \rangle \subseteq J/I = \bar{J}$ is clear. On the other hand, if we take an element $x + I \in J/I$ where $x \in J$, we can find $a_1, \ldots, a_n \in A$ such that $x = a_1 x_1 + \cdots + a_n x_n$. Then one sees that

$$x + I = (a_1 + I)(x_1 + I) + \cdots + (a_n + I)(x_n + I) \in \langle x_1 + I, \ldots, x_n + I \rangle.$$

2. Let $\alpha := \sqrt{1 + \sqrt{3}}$. Find the minimal polynomial of α over $\mathbb{Q}$.

Notice $\alpha^2 = 1 + \sqrt{3}$, and therefore we have

$$3 = (\alpha^2 - 1)^2 = \alpha^4 - 2\alpha^2 + 1,$$

and thus α is a root of $x^4 - 2x^2 - 2$. One sees this polynomial is irreducible in $\mathbb{Q}[x]$ with Eisenstein's criterion and therefore it is the minimal polynomial of α over $\mathbb{Q}$.

3. Suppose $f(x)$ and $g(x)$ are monic integer polynomials. Prove that $f(x)|g(x)$ in $\mathbb{Q}[x]$ if and only if $f(x)|g(x)$ in $\mathbb{Z}[x]$.

Clearly if $f(x)|g(x)$ in $\mathbb{Z}[x]$, then $f(x)|g(x)$ in $\mathbb{Q}[x]$. On the other hand suppose $f(x)|g(x)$ in $\mathbb{Q}[x]$, say $g(x) = f(x)q(x)$ for some $q(x) \in \mathbb{Q}[x]$. By Gauss's lemma we have $\alpha(g) = \alpha(f)\alpha(q)$, but $\alpha(g) = \alpha(f) = 1$ by our hypotheses, so $\alpha(q) = 1$, and from the definition of content one sees this implies that $q(x) \in \mathbb{Z}[x]$.

4. Suppose n is a positive odd integer. Prove that $f(x) = (x-1)(x-2)\cdots(x-n) - 1$ is irreducible in $\mathbb{Q}[x]$. (Hint. Assume the contrary and first reduce it to the case where $f(x) = g(x)h(x)$ for some non-constant integer polynomials $g(x)$ and $h(x)$. Then consider $f(i)$ for integer i in $[1, n]$, and think about $g(x)^2 - 1$ and $h(x)^2 - 1$.)

Suppose $f(x)$ is not irreducible in $\mathbb{Q}[x]$, say $f(x) = g(x)h(x)$ for some non-constant $g, h \in \mathbb{Q}[x]$. Using Theorem 11.3.1 one can reduce to the case where $g, h \in \mathbb{Z}[x]$. Because $\deg(g) + \deg(h) = \deg(f) = n$ is odd, we have $\deg(g) \neq \deg(h)$, say without loss of generality $\deg(g) < \deg(h)$. Then one sees that

$$2\deg(g) < \deg(g) + \deg(h) = \deg(f) = n.$$

Now notice for any $i \in \{1, 2, \ldots, n\}$, we have $f(i) = -1$, so $g(i) = \pm 1$. As a result we see that the polynomial $g(x)^2 - 1$ vanishes at each $i \in \{1, \ldots, n\}$, so it has at least n distinct roots. But g is non-constant which implies $g(x)^2 - 1$ is non-constant of degree $2\deg(g) < n$, and comparing with the fact that $g(x)^2 - 1$ has n distinct roots we have a contradiction.

5. Suppose p is prime, $f(x) \in \mathbb{Z}_p[x]$ is irreducible, and $n := \deg f$.
   (a) Let $F := \mathbb{Z}_p[x]/\langle f(x)\rangle$. Prove that F is a field of order p^n, which contains a copy of $\mathbb{Z}_p$.

   Recall that $\mathbb{Z}_p[x]$ is a PID because $\mathbb{Z}_p$ is a field. Thus the fact that $f(x)$ is irreducible in $\mathbb{Z}_p[x]$ implies that $\langle f(x)\rangle$ is a maximal ideal of $\mathbb{Z}_p[x]$, and then $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field. To see it has order p^n one can apply Homework 4, Problem 1.

   (b) Prove that $\alpha := x + \langle f(x)\rangle$ is a zero of $f(X) \in \mathbb{Z}_p[X] \subseteq F[X]$ (we consider the coefficients as elements of the copy of $\mathbb{Z}_p$ in F).

   Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ where $a_i \in \mathbb{Z}_p$. Written as an element of $F[X]$ we have $f(X) = (a_0 + \langle f(x)\rangle) + (a_1 + \langle f(x)\rangle)X + \cdots + (a_n + \langle f(x)\rangle)X^n$. Plugging in α we calculate

$$\begin{aligned} f(\alpha) &= f(x + \langle f(x)\rangle) \\ &= (a_0 + \langle f(x)\rangle) + \cdots + (a_n + \langle f(x)\rangle)(x + \langle f(x)\rangle)^n \\ &= (a_0 + a_1 x + \cdots + a_n x^n) + \langle f(x)\rangle \\ &= f(x) + \langle f(x)\rangle \\ &= 0 + \langle f(x)\rangle \\ &= 0_F. \end{aligned}$$

   This shows α is a zero of f.

   (c) Prove that $\alpha^{p^n} = \alpha$. (Hint: for $\alpha \neq 0$, consider the group $F^\times$ of units of F.)

   If $\alpha = 0$ then the result holds. If $\alpha \neq 0$ then $\alpha \in F^\times$, which is a group of order $p^n - 1$ under multiplication. Thus Lagrange's theorem tells us that $\alpha^{p^n - 1} = 1$, and multiplying by α gives the result.

   (d) Prove that $f(X) | X^{p^n} - X$ in $\mathbb{Z}_p[X]$.

   Notice α is a root of $X^{p^n} - X$ by part (c), and therefore $m_{\alpha,\mathbb{Z}_p}(X) | X^{p^n} - X$ in $\mathbb{Z}_p[x]$. But also notice that $\frac{1}{a_n} f(X)$ is a monic irreducible polynomial in $\mathbb{Z}_p[X]$ with α as a root, and hence $\frac{1}{a_n} f(X) = m_{\alpha,\mathbb{Z}_p}(X)$. As a result one sees that $f(X) | X^{p^n} - X$ in $\mathbb{Z}_p[X]$ as well.

7. Week 7

(Thanks to Alex Mathers for providing most of these solutions.)

1. Suppose D is a UFD, and $Q(D)$ is the field of fractions of D. For $f(x) \in Q(D)[x]$, let $\bar{f}(x) := \text{prim}(f)$ be the primitive form of f. Prove $f \in Q(D)[x]$ is irreducible if and only if $\bar{f}$ is irreducible in $D[x]$.

   Suppose f is reducible in $Q(D)[x]$, say $f(x) = g(x)h(x)$ for non-constant $g, h \in Q(D)[x]$. Then because the prim function is multiplicative, we have $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ where $\bar{g}, \bar{h}$ are the primitive forms of g, h. Because $\deg(\bar{g}) = \deg(g)$ and $\deg(\bar{h}) = \deg(h)$, we see that $\bar{f}(x)$ is a product of non-constant polynomials in $D[x]$, in particular it is a product of non-units in $D[x]$, so it is reducible as well.

   Now suppose $\bar{f}$ is reducible in $D[x]$, say $\bar{f}(x) = p(x)q(x)$ for some non-units $p, q \in D[x]$ (remark: we cannot immediate say from the definition that $\bar{f}(x)$ is a product of non-constant polynomials, think about $2x$ in $\mathbb{Z}[x]$). Then by Gauss's lemma we have $\alpha(\bar{f}) = \alpha(p)\alpha(q)$, and $\alpha(\bar{f}) = 1$ because $\bar{f}$ is primitive. Since $p, q \in D[x]$, we have $\alpha(p), \alpha(q) \in D$, so $\alpha(p)\alpha(q) = 1$ tells us that $\alpha(p)$ and $\alpha(q)$ are units in D, i.e. p and q are primitive polynomials. Now if one of them were constant, say p constant, then we'd have $p(x) = \alpha(p) \in D^\times$, contradicting the fact that p, q are non-units in $D[x]$. Thus p and q are non-constant, and then we have a factorization

$$f(x) = \alpha(f)\bar{f}(x) = \alpha(f)p(x)q(x) = (\alpha(f)p(x))q(x)$$

   which shows that f factors into a product of non-constant polynomials in $Q(D)[x]$, so it is reducible.

2. Prove that $\mathbb{C}[x, y]/\langle x^n + y^n - 1\rangle$ is an integral domain.

   The quotient $\mathbb{C}[x, y]/\langle x^n + y^n - 1\rangle$ is an integral domain if and only if the ideal $\langle x^n + y^n - 1\rangle$ is a prime ideal of $\mathbb{C}[x, y]$. This ideal is prime if and only if the element $x^n + y^n - 1$ is a prime element of $\mathbb{C}[x, y]$, and because $\mathbb{C}[x, y]$ is a UFD this is the same as being an irreducible element of $\mathbb{C}[x, y]$. As a first step to show $x^n + y^n - 1$ is irreducible in $\mathbb{C}[x, y]$, we will view it as a polynomial in $(\mathbb{C}[y])[x]$ and apply Eisenstein's criterion (remark: notice we can apply Eisenstein's criterion because $\mathbb{C}[y]$ is a UFD). As an element of $(\mathbb{C}[y])[x]$, it is equal to $x^n + (y^n - 1)$, i.e. it is monic with constant term $y^n - 1 \in \mathbb{C}[y]$; we need to find a prime element $p \in \mathbb{C}[y]$ such that $p|(y^n - 1)$ and $p^2 \nmid (y^n - 1)$. For this we take $p = y - 1$. One has $y^n - 1 = (y - 1)(y^{n-1} + \cdots + y + 1)$ in $\mathbb{C}[x, y]$, so $(y - 1)|(y^n - 1)$, and because $y^{n-1} + \cdots + y + 1$ does not have a root at 1, we see by the factor theorem that $(y - 1) \nmid (y^{n-1} + \cdots + y + 1)$, so $(y - 1)^2 \nmid (y^n - 1)$. Thus the conditions for Eisenstein's criteria are satisfied for $D = \mathbb{C}[y]$ and $p = y - 1$.

   The result of Eisenstein's criterion is that $x^n + (y^n - 1)$ cannot be written as a product of polynomials of smaller degree in $(\mathbb{C}[y])[x]$. Now suppose we have a factorization $x^n + y^n - 1 = f(x, y)g(x, y)$ for $f, g \in \mathbb{C}[x, y]$. Then viewing these as elements of $(\mathbb{C}[y])[x]$, because $x^n + y^n - 1$ cannot be written as a product of polynomials of smaller degree in $(\mathbb{C}[y])[x]$, one of the two must be constant, without loss of generality say f is constant (remark: this does not mean $f \in \mathbb{C}$; we mean f is constant as a polynomial in $(\mathbb{C}[y])[x]$, so $f \in \mathbb{C}[y]$). By comparing leading coefficients (i.e. the leading terms in as polynomials in x, because we are viewing these as elements of $(\mathbb{C}[y])[x]$), because $x^n + (y^n - 1)$ is monic we deduce that $f \in \mathbb{C}[y]^\times = \mathbb{C}$; but then f is a unit in $\mathbb{C}[x, y]$ so this shows $x^n + y^n - 1$ is irreducible.

   Remark. Here is the right generalization of Eisenstein's irreducibility criterion as it is formulated in Theorem 12.2.1.

Theorem (Eisenstein's criterion for UFDs). *Suppose D is a UFD, $f(x) := a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ and $p \in D$ is prime. If*

$$p \nmid a_n, p|a_{n-1}, \ldots, p|a_0, \text{ and } p^2 \nmid a_0,$$

then f is irreducible in $Q(D)[x]$.

Combining Eisenstein's irreducibility criterion for UFDs and problem 1 imply that if a *monic* polynomial satisfies the conditions of Eisenstein's irreducibility criterion, then it is irreducible in $D[x]$. For future reference, you are allowed to use these formulations after carefully stating them.

3. Prove that $x^3 + 12x^2 + 18x + 6$ is irreducible in $(\mathbb{Z}[i])[x]$.

We again use Eisenstein's criterion for UFDs: our coefficient ring is $D = \mathbb{Z}[i]$ (which is a UFD because we have proved it is a PID), and we will take $p = 3$ as our prime element. First we need to show this is actually a prime element: recall the norm function $N : \mathbb{Z}[i] \to \mathbb{Z}^{\geq 0}$, $N(z) := |z|^2$ is multiplicative, and that $N(z) = 1 \iff z \in \mathbb{Z}[i]^\times$. We first notice that $N(3) = 9 \neq 1$, so $3 \notin \mathbb{Z}[i]^\times$, and clearly 3 is non-zero, so $3 \notin \mathbb{Z}[i]^\times \cup \{0\}$.

Now suppose $3 = xy$ for elements $x, y \in \mathbb{Z}[i]$. We have $9 = N(3) = N(xy) = N(x)N(y)$, and we claim we cannot have $N(x) = N(y) = 3$; if this were the case then, writing $x = a + bi$ for $a, b \in \mathbb{Z}$, we would have

$$3 = N(x) = N(a + bi) = a^2 + b^2,$$

but notice 3 cannot be written as the sum of two squares in $\mathbb{Z}$ so this is impossible. Thus from $N(x)N(y) = 9$ we have that either $N(x) = 1$ or $N(y) = 1$, and so either x or y is a unit in $\mathbb{Z}[i]$, showing 3 is irreducible in $\mathbb{Z}[i]$.

Now we can continue with our proof: we wish to invoke Eisenstein's criterion for the polynomial $x^3 + 12x^2 + 18x + 6$ and the prime element $p = 3$ in $\mathbb{Z}[i]$; clearly 3 divides all the coefficients except the leading term, and we need to see that $3^2 \nmid 6$ in $\mathbb{Z}[i]$: but if $9|6$ in $\mathbb{Z}[i]$, then using multiplicativity of the norm function one would have $N(9)|N(6)$ in $\mathbb{Z}$, i.e. $81|36$ in $\mathbb{Z}$, which we know does not hold. Thus the conditions of Eisenstein's irreducibility criterion hold. Since this is monic polynomial, by the remark made at the end of the previous problem, we deduce that it is an irreducible element of $(\mathbb{Z}[i])[x]$.

Alternatively we can avoid using the above mentioned remark and continue as follows:

Thus we can invoke Eisenstein's criterion to tell us that $x^3 + 12x^2 + 18x + 6$ cannot be written as a product of polynomials of smaller degree in $(\mathbb{Z}[i])[x]$. We are not quite done: one needs to note that if $x^3 + 12x^2 + 18x + 6 = f(x)g(x)$ for $f, g \in (\mathbb{Z}[i])[x]$, then we know one of the terms must be constant, but then by comparing leading coefficients whichever polynomial is constant would then be a unit in $\mathbb{Z}[i]$, and thus we see that $x^3 + 12x^2 + 18x + 6$ is irreducible in $(\mathbb{Z}[i])[x]$.

Remark. One can repeat the above argument and show that if p is a prime integer and $p \equiv 3 \pmod 4$, then p is irreducible in $\mathbb{Z}[i]$. As before, we can see that p is neither zero nor a unit. Suppose $p = ab$ for some $a, b \in \mathbb{Z}[i]$. This implies that $p^2 = N(a)N(b)$. Hence by a similar argument as above it is sufficient to show that there is no $a \in \mathbb{Z}[i]$ such that $N(a) = p$. Suppose to the contrary that there are integers x and y such that $N(x + iy) = p$. This means $p = x^2 + y^2$. Considering both sides modulo 4, we deduce that $x^2 + y^2 \equiv 3 \pmod 4$. Notice that for every integer z, we have that z^2 is either 0 or 1 modulo 4. Hence $x^2 + y^2$ can never be 3 modulo 4. This gives us the needed contradiction (From this point on you are allowed to use this fact if needed.).

4. Suppose D is a PID. Prove that every non-zero prime ideal is maximal.

If I is a non-zero prime ideal of D, then because D is a PID we must have $I = \langle p \rangle$ for some element $p \in D$. Now I non-zero implies that $p \neq 0$, and then the fact that I is prime implies that p is a prime element of D. But then p is an irreducible element of D (prime elements are always irreducible in

an integral domain), and then because D is a PID this implies that $I = \langle p \rangle$ is a maximal ideal of D.

5. Suppose D is a UFD, and $\langle a, b \rangle = \langle \gcd(a, b) \rangle$ for every $a, b \in D \setminus \{0\}$.
   (a) Prove that every finitely generated ideal of D is principal.

First we notice (remark: this means if the following equality is not clear to you, then prove it yourself before moving on!) that if we are given elements $x_1, \ldots, x_n, y_1, \ldots, y_m$ of D, then

$$\langle x_1, \ldots, x_n, y_1, \ldots, y_m \rangle = \langle x_1, \ldots, x_n \rangle + \langle y_1, \ldots, y_m \rangle.$$

We prove by induction on n that any ideal generated by n elements, i.e. an ideal of the form $\langle x_1, \ldots, x_n \rangle$, is principal. The base case $n = 1$ is trivial. So we focus on the induction step; that means we assume that the result is true for an integer n, show that an ideal generated by $n+1$ elements is principal as well. For an ideal $\langle x_1, \ldots, x_{n+1} \rangle$, by the induction hypothesis we have that $\langle x_1, \ldots, x_n \rangle$ is principal, say $\langle x_1, \ldots, x_n \rangle = \langle y \rangle$. We then calculate

$$\begin{aligned} \langle x_1, \ldots, x_{n+1} \rangle &= \langle x_1, \ldots, x_n \rangle + \langle x_n \rangle \\ &= \langle y \rangle + \langle x_{n+1} \rangle \\ &= \langle y, x_{n+1} \rangle \\ &= \langle \gcd(y, x_{n+1}) \rangle. \end{aligned}$$

Thus $\langle x_1, \ldots, x_{n+1} \rangle$ is principal and we have the result by induction on n.

   (b) For every non-zero non-unit element a of D, $\{\langle d \rangle \mid d|a\}$ is a finite set.

Because a is non-zero and a non-unit, it has a factorization into irreducible elements $a = \prod_{p \in \mathcal{P}_D} p^{v_p(a)}$. If $d|a$, then by the unique factorization one has that $v_p(d) \leq v_p(a)$ for all $p \in \mathcal{P}_D$. In particular we have $d = u \prod_{p \in \mathcal{P}_D} p^{n_p}$ for some integers $0 \leq n_p \leq v_p(a)$ and some unit $u \in D^\times$, and then

$$\langle d \rangle = \langle u \prod_{p \in \mathcal{P}_D} p^{n_p} \rangle = \langle \prod_{p \in \mathcal{P}_D} p^{n_p} \rangle.$$

Thus we see every ideal $\langle d \rangle$ for $d|a$ has the form $\langle \prod_{p \in \mathcal{P}_D} p^{n_p} \rangle$ for some integers $0 \leq n_p \leq v_p(a)$. Because $v_p(a) = 0$ for all but finitely many $p \in \mathcal{P}_D$, we see that the set of such ideals $\langle \prod_{p \in \mathcal{P}_D} p^{n_p} \rangle$ for $0 \leq n_p \leq v_p(a)$ is finite, so the set $\{\langle d \rangle \mid d|a\}$ is finite.

   (c) Prove that D is a PID.

Solution 1. By part (a) every finitely generated ideal is principal, so we just need to show that every ideal of D is finitely generated. To the contrary, suppose we have an ideal $I \lhd D$ which is not finitely generated. Notice that $\{0\}$ is finitely generated, so we have $I \neq \{0\}$; thus we can choose some element $a_1 \in I \setminus \{0\}$. We then have $\langle a_1 \rangle \subseteq I$, but the two cannot be equal because this would mean that I is finitely generated; thus we can choose an element $a_2 \in I \setminus \langle a_1 \rangle$. Continuing this process, for each n we can choose $a_{n+1} \in I \setminus \langle a_1, \ldots, a_n \rangle$, at each step using the fact that I is not finitely generated. This gives is an infinite ascending chain of strict inclusions

$$\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \cdots.$$

But by part (a) we know that every finitely generated ideal is principal, so for each n we can write $\langle a_1, \ldots, a_n \rangle = \langle d_n \rangle$ for some $d_n \in D$. The our ascending chain can be rewritten as

$$\langle a_1 \rangle \subsetneq \langle d_2 \rangle \subsetneq \langle d_3 \rangle \subsetneq \cdots.$$

But for each n, the fact that $\langle a_1 \rangle \subseteq \langle d_n \rangle$ implies that $d_n | a_1$. Thus $\{\langle d_n \rangle \mid n \geq 2\} \subseteq \{\langle d \rangle \mid d|a\}$. Notice the set on the left is infinite because our ascending chain is infinite with strict inclusions.

On the other hand, notice a_1 is non-zero by choice, and also a_1 is not a unit (if it were a unit then $a_1 \in I$ would imply that $I = D = \langle 1 \rangle$ which is finitely generated), so we can invoke part (b) to see that the set on the right is finite, giving a contradiction.

Solution 2. By part (a) every finitely generated ideal is principal, so we just need to show that every ideal of D is finitely generated. Suppose I is an ideal of D. If I is the 0 ideal or D, then it is clearly principal. So without loss of generality we can and will assume that I is a non-zero proper ideal. Hence there is $a_0 \in I$ which is not zero and non-unit. By part (b), there are finitely many divisors $d_1, \ldots, d_k$ of a_0 such that

$$\{\langle d \rangle \mid d | a_0\} = \{\langle d_1 \rangle, \ldots, \langle d_k \rangle\}. \tag{19}$$

For every $b \in I$, by hypothesis, $\langle a_0, b \rangle = \langle \gcd(a_0, b) \rangle$. Hence by (19), there is an index $i(b)$ which depends on b such that

$$\langle a_0, b \rangle = \langle d_{i(b)} \rangle.$$

Claim. $\langle d_{i(b)} \mid b \in I \rangle = I$. In particular, I is finitely generated.
Proof of Claim. Let $J := \langle d_{i(b)} \mid b \in I \rangle$. Then, for every $b \in I$, $b \in \langle a_0, b \rangle = \langle d_{i(b)} \rangle$. Hence b is a multiple of $d_{i(b)}$, which implies that b is in J. Therefore $I \subseteq J$. For every $b \in I$, $d_{i(b)} \in \langle a_0, b \rangle \subseteq I$. Hence $d_{i(b)}$'s are in I. Therefore $J \subseteq I$ as J is generated by $d_{i(b)}$'s.

8. Week 8

(Thanks to Alex Mathers for providing these solutions.)

1. This is an exercise from math100a which gives us a characterization of cyclic groups.
   (a) Suppose $C_n := \{1, a, \ldots, a^{n-1}\}$ is a cyclic group of order n. Show that if $d|n$, then C_n has exactly $\phi(d)$ elements of order d. Use this to conclude that

$$\sum_{d|n} \phi(d) = n.$$

Let $d|n$. Recall that, because C_n is a cyclic group, it has a unique subgroup of order d, call it H. Now by the uniqueness of this subgroup we see that for an element $x \in C_n$ we have

$$o(x) = d \iff |\langle x \rangle| = d \iff \langle x \rangle = H.$$

So it suffices to count the number of elements which generate H. But H is a cyclic group of order d, so from 100a we know H has $\phi(d)$ generators (see the extra remark at the end of the solution to recall why this holds), and thus C_n has $\phi(d)$ elements of order d. Now the final equality follows by noting that every element of C_n has order d for some $d|n$, leading us to the equality of sets

$$\coprod_{d|n} \{x \in C_n \mid o(x) = d\} = C_n,$$

upon which taking cardinalities produces the desired equality.

Remark: let $H = \langle x \rangle$ be a cyclic group of order d. Then any element of H has the form x^m for some $1 \leq m < d$, and we recall from 100a that

$$o(x^m) = \frac{o(x)}{\gcd(o(x), m)} = \frac{d}{\gcd(d, m)}.$$

Thus we get $o(x^m) = d \iff \gcd(d, m) = 1$, and so the number of elements of order d (i.e. the number of generators of H) is exactly the number of $m \in \{1, \ldots, d-1\}$ such that $\gcd(d, m) = 1$, i.e. equal to $\phi(d)$.

(b) Suppose G is a finite group and for every positive integer d,

$$|\{g \in G \mid g^d = 1\}| \leq d.$$

Prove that G is cyclic.

Let $\psi(d)$ denote the number of elements of G of order d. If we are given an element $g \in G$ of order d, then $1, g, \ldots, g^{d-1}$ are distinct elements of G all satisfying $x^d = 1$. By the hypothesis then we see that $1, g, \ldots, g^{d-1}$ are the only elements of G satisfying $x^d = 1$; the elements which have order d are then exactly the powers g^m where $\gcd(d, m) = 1$ (for example see our remark at the end of the previous solution). Overall we see that if $\psi(d) \neq 0$, i.e. if G has an element of order d, then we can follow the above argument and find that there are exactly $\phi(d)$ elements of order d, so $\psi(d) = \phi(d)$ in this case.

Now letting $n = |G|$ we have that $n = \sum_{d|n} \psi(d)$, for instance by taking the same partition as in part (a), i.e. $G = \coprod_{d|n} \{x \in G \mid o(x) = d\}$, and taking cardinalities. Now we also know from part (a) that $n = \sum_{d|n} \phi(d)$. We claim from this we can deduce that $\psi(d) \neq 0$ for any $d|n$. For a contradiction suppose $\psi(d_0) = 0$ for some $d_0|n$; then we calculate

$$n = \sum_{d|n} \psi(d) = \sum_{\substack{d|n \\ \psi(d)\neq 0}} \psi(d) = \sum_{\substack{d|n \\ \psi(d)\neq 0}} \phi(d) \leq \sum_{\substack{d|n \\ d\neq d_0}} \phi(d) < \sum_{d|n} \phi(d) = n.$$

Notice the third equality follows from the fact that $\psi(d) = \phi(d)$ whenever $\psi(d) \neq 0$, and the strict inequality follows because $\phi(d_0) \neq 0$. Overall we obtain $n < n$, a contradiction; we deduce that $\psi(d) \neq 0$ for any $d|n$, and in particular we can take $d = n$ to find that $\psi(n) \neq 0$, i.e. G has an element of order n, so G is cyclic.

2. Suppose F is a finite field. Prove that $F^\times$ is cyclic. Deduce that $x^2 = -1$ has a solution in a finite field F of odd characteristic if and only if $|F| \equiv 1 \pmod 4$.

We apply 1(b) for $G = F^\times$; because $x^d - 1$ has at most d roots in F, we get

$$|\{\alpha \in F^\times \mid \alpha^d = 1\}| \leq d$$

for any positive integer d, and we deduce from Problem 1(b) that $F^\times$ is cyclic.

For the second part, we start with the claim that an element $\alpha \in F$ satisfies $\alpha^2 = -1$ if and only if $o(\alpha) = 4$ in the multiplicative group $F^\times$. On one hand if $\alpha^2 = -1$ then $\alpha^2 \neq 1$ (note that $-1 \neq 1$ because $\mathrm{char}(F) \neq 2$) but $\alpha^4 = 1$, so we see $o(\alpha) = 4$; conversely if $o(\alpha) = 4$ then $\alpha^2 \neq 1$ but α^2 is a root of $x^2 - 1 = (x + 1)(x - 1)$, and this implies $\alpha^2 = -1$. Now with this proven, we recall that because $F^\times$ is a cyclic group, it contains an element of order d if and only if d divides $|F^\times| = |F| - 1$. Putting these facts together we have

$$\begin{aligned} x^2 = -1 \text{ has a solution in } F &\iff \text{there exists } \alpha \in F^\times \text{ of order } 4 \\ &\iff 4 \text{ divides } |F^\times| = |F| - 1 \\ &\iff |F| \equiv 1 \pmod 4. \end{aligned}$$

3. Suppose F is a splitting field of $x^n - 1$ over $\mathbb{Z}_3$.
(a) Find $|F|$ if $n = 3$.

Notice $x^3 - 1 = (x - 1)^3$ in $\mathbb{Z}_3[x]$. Thus $x^3 - 1$ splits into linear factors in $\mathbb{Z}_3[x]$, and one sees that $\mathbb{Z}_3$ satisfies the conditions for a splitting field of $x^3 - 1$ over $\mathbb{Z}_3$, so $|F| = |\mathbb{Z}_3| = 3$.

(b) Find $|F|$ if $n = 13$.

We claim that $\mathbb{F}_{27}$ is a splitting field for $x^{13} - 1$ over $\mathbb{Z}_3$. Notice that 13 divides $\mathbb{F}_{27}^\times$ and $\mathbb{F}_{27}^\times$ is cyclic, so there is a subgroup $H \leq \mathbb{F}_{27}^\times$ of order 13. Then by Lagrange's theorem every element of H is a root of $x^{13} - 1$, and because $|H| = 13$ we see that $x^{13} - 1$ splits into linear factors in $\mathbb{F}_{27}[x]$, with roots exactly the elements of H. Let $\alpha_1, \ldots, \alpha_{13}$ denote the roots of $x^{13} - 1$ in $\mathbb{F}_{27}$, i.e. the elements of H. Then we consider the subfield $F := \mathbb{Z}_3[\alpha_1, \ldots, \alpha_{13}] \subseteq \mathbb{F}_{27}$ which is a splitting field of $x^{13} - 1$ over $\mathbb{Z}_3$.

Now we claim that $|F| = 27$. Because F is a field extension of $\mathbb{Z}_3$ and contained in $\mathbb{F}_{27}$, the possible orders of F are $3, 9$, or 27 (the order must be a power of 3). But notice that $H \leq F^\times$ by construction, so $|H|$ divides $|F^\times| = |F| - 1$, and this rules out 3 and 9. Thus $|F| = 27$.

(c) Find $|F|$ if $n = 39$.

Notice that $x^{39} - 1 = (x^{13} - 1)^3$ in $\mathbb{Z}_3[x]$, which implies that the splitting field of $x^{39} - 1$ over $\mathbb{Z}_3$ equals the splitting field of $x^{13} - 1$ over $\mathbb{Z}_3$, so by part (b) we have $|F| = 27$.

4. Suppose p is prime and $\zeta_p := e^{2\pi i/p}$.

(a) Prove that for every integer j in $[1, p-1]$, there is an isomorphism $\theta_j : \mathbb{Q}[\zeta_p] \to \mathbb{Q}[\zeta_p]$ such that $\theta_j(\zeta_p) = \zeta_p^j$.

Recall $1, \zeta_p, \ldots, \zeta_p^{p-1}$ are the roots of $x^p - 1$ in $\mathbb{C}$, and from $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$ we see that $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ are the roots of $x^{p-1} + \cdots + x + 1$ in $\mathbb{C}$, and we know this polynomial is irreducible in $\mathbb{Q}[x]$. Thus from Lemma 16.2.2 for each integer $j \in [1, p-1]$ there exists some isomorphism $\theta_j : \mathbb{Q}[\zeta_p] \to \mathbb{Q}[\zeta_p^j] = \mathbb{Q}[\zeta_p]$ such that $\theta_j(\zeta_p) = \zeta_p^j$.

Remark: We used here that $\mathbb{Q}[\zeta_p] = \mathbb{Q}[\zeta_p^j]$. To prove this, first we clearly have $\mathbb{Q}[\zeta_p^j] \subseteq \mathbb{Q}[\zeta_p]$; conversely notice that, because j is coprime to p we can find $a, b \in \mathbb{Z}$ with $aj + bp = 1$. Then

$$\zeta_p = \zeta_p^{aj+bp} = (\zeta_p^j)^a (\zeta_p^p)^b = (\zeta_p^j)^a \in \mathbb{Q}[\zeta_p^j].$$

(b) Prove that if $\theta : \mathbb{Q}[\zeta_p] \to \mathbb{Q}[\zeta_p]$ is an isomorphism, then $\theta = \theta_j$ for some integer j in $[1, p-1]$.

Let $\theta : \mathbb{Q}[\zeta_p] \to \mathbb{Q}[\zeta_p]$. Because ζ_p is a root of $x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x]$ and θ must fix elements of $\mathbb{Q}$ (i.e. $\theta(a) = a$ for $a \in \mathbb{Q}$), we have that $\theta(\zeta_p)$ must be a root of $x^{p-1} + \cdots + x + 1$. But we showed in part (a) that the roots of this polynomial are exactly $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$, and so $\theta(\zeta_p) = \zeta_p^j = \theta_j(\zeta_p)$ for some integer $j \in [1, p-1]$. We claim this implies that $\theta = \theta_j$. To see this, we take an arbitrary element of $\mathbb{Q}[\zeta_p]$, which must have the form $\sum_{i=0}^{p-2} a_i \zeta_p^i$ for $a_i \in \mathbb{Q}$. Then using the fact that θ and θ_j are ring homomorphisms we compute

$$\theta\Big(\sum_{i=0}^{p-2} a_i \zeta_p^i\Big) = \sum_{i=0}^{p-2} a_i \, \theta(\zeta_p)^i = \sum_{i=0}^{p-2} a_i \, \theta_j(\zeta_p)^i = \theta_j\Big(\sum_{i=0}^{p-2} a_i \zeta_p^i\Big).$$

Because this element was arbitrary we conclude $\theta = \theta_j$.

9. Week 9

(Thanks to Alex Mathers for providing these solutions.)

1. Suppose $f(x) \in F[x]$ is irreducible. Let E be a splitting field of f over F. Let $\alpha \in E$ be a zero of F. Prove that

$$|\operatorname{Emb}_F(F[\alpha], E)| = \text{number of distinct zeros of } f \text{ in } E.$$

We show in fact that we have a bijection

$$\mathrm{Emb}_F(F[\alpha], E) \to \{\text{zeros of } f \text{ in } E\}$$

given by sending $\theta \mapsto \theta(\alpha)$. This map makes sense because any $\theta \in \mathrm{Emb}_F(F[\alpha], E)$ must send zeros of f to zeros of f. For surjectivity we need to see that for any zero α' of f, there is an element $\theta \in \mathrm{Emb}_F(F[\alpha], E)$ such that $\theta(\alpha) = \alpha'$. For any such α' we have the subfield $F[\alpha'] \subseteq E$, and we know because f is irreducible that there is an isomorphism $F[\alpha] \to F[\alpha']$ sending $\alpha \mapsto \alpha'$, and then we take θ to be the composition $F[\alpha] \to F[\alpha'] \hookrightarrow E$ where the latter map is the inclusion map.

Now we need to show injectivity, i.e. we need to show that given $\theta, \theta' \in \mathrm{Emb}_F(F[\alpha], E)$ such that $\theta(\alpha) = \theta'(\alpha)$, then $\theta = \theta'$. For this we first write $f(x) = c_0 + \cdots + c_n x^n$ for $c_i \in F$. Then we take an arbitrary element of $F[\alpha]$, which has the form $\sum_{i=0}^{n-1} c_i \alpha^i$ for some $c_i \in F$. Now using the fact that θ, θ' are ring homomorphisms and $\theta(c_i) = c_i = \theta'(c_i)$ for each i we calculate

$$\theta\big(\sum_{i=0}^{n-1} c_i \alpha^i\big) = \sum_{i=0}^{n-1} c_i\, \theta(\alpha)^i = \sum_{i=0}^{n-1} c_i\, \theta'(\alpha)^i = \theta'\big(\sum_{i=0}^{n-1} c_i \alpha^i\big).$$

Thus $\theta = \theta'$, which completes the proof of injectivity, and hence the proof that our map is a bijection.

2. Suppose F is a field and E is a splitting field of $g(x) \in F[x] \setminus F$ over F.
   (a) Suppose L is a field extension of E. Prove that, for every $\theta \in \mathrm{Emb}_F(E, L)$, $\theta(E) = E$.

Let $\beta_1, \ldots, \beta_m$ be the roots of $g(x)$ in E, so by hypothesis $E = F[\beta_1, \ldots, \beta_m]$. We know that for each i, $\theta(\beta_i)$ is a root of $g(x)$, so $\theta(\beta_i) = \beta_j$ for some j. Thus θ restricts to a function $\{\beta_1, \ldots, \beta_m\} \to \{\beta_1, \ldots, \beta_m\}$, and because θ is injective this restriction is also surjective as well, i.e. θ restricts to a permutation of the set of roots. Using this fact, and the F-linearity of θ we have

$$\theta(E) = \theta(F[\beta_1, \ldots, \beta_m]) = F[\theta(\beta_1), \ldots, \theta(\beta_m)] = F[\beta_1, \ldots, \beta_m] = E.$$

Remark: if one finds the above line unsatisfying, we can be more precise: on one hand, any element of E has the form of a finite sum $\sum_{i_1,\ldots,i_m} c_{i_1\cdots i_m} \beta_1^{i_1} \cdots \beta_m^{i_m}$ for some nonnegative integers i_j, and then

$$\theta\big(\sum_{i_1,\ldots,i_m} c_{i_1\cdots i_m} \beta_1^{i_1} \cdots \beta_m^{i_m}\big) = \sum_{i_1,\ldots,i_m} c_{i_1\cdots i_m} \theta(\beta_1)^{i_1} \cdots \theta(\beta_m)^{i_m},$$

which is an element of E because each coefficient $c_{i_1\cdots i_m} \in E$ and $\theta(\beta_j) \in E$ for each j. On the other hand recall $E = F[\beta_1, \ldots, \beta_m]$ is the smallest subring of E containing F and $\beta_1, \ldots, \beta_m$. But we have $\beta_j \in \theta(E)$ and $F \subseteq \theta(E)$, so it follows that $\theta(E)$ is a subring of E containing F and $\beta_1, \ldots, \beta_m$, thus $E \subseteq \theta(E)$ as well, giving $\theta(E) = E$.

   (b) Suppose $\alpha \in E$, and let L be a splitting field of $m_{\alpha,F}(x)$ over E. Prove L is a splitting field of $m_{\alpha,F}(x)g(x)$ over F.

We retain notation from the previous solution, so $E = F[\beta_1, \ldots, \beta_m]$ where the $\{\beta_i\}$ are the roots of $g(x)$ in E. We let $\alpha_1, \ldots, \alpha_n$ denote the roots of $m_{\alpha,F}$ in L; then by hypothesis $L = E[\alpha_1, \ldots, \alpha_n]$. Now in $L[x]$ we have

$$m_{\alpha,F}(x)g(x) = (x - \alpha_1) \cdots (x - \alpha_n)(x - \beta_1) \cdots (x - \beta_m),$$

and in addition

$$L = E[\alpha_1, \ldots, \alpha_n] = (F[\beta_1, \ldots, \beta_n])[\alpha_1, \ldots, \alpha_n] = F[\beta_1, \ldots, \beta_m, \alpha_1, \ldots, \alpha_n].$$

This shows L is a splitting field of $m_{\alpha,F}(x)g(x)$ over F.

(c) Suppose $\alpha \in E$, and let L be a splitting field of $m_{\alpha,F}(x)$ over E. Let $\alpha' \in L$ be a zero of $m_{\alpha,F}(x)$. Prove that there is $\widehat{\theta} \in \mathrm{Emb}_F(L, L)$ such that $\widehat{\theta}(\alpha) = \alpha'$.

Consider the subfields $F[\alpha]$ and $F[\alpha']$ of L. We know because $m_{\alpha,F}(x)$ is irreducible in $F[x]$, there exists an F-linear isomorphism $\theta : F[\alpha] \to F[\alpha']$ such that $\theta(\alpha) = \alpha'$. We know by part (b) that L is a splitting field of $m_{\alpha,F}(x)g(x)$ over F, so L is also a splitting field of $m_{\alpha,F}(x)g(x)$ over both $F[\alpha]$ and $F[\alpha']$. Thus we can invoke Theorem 17.1.1 to find an an isomorphism $\widehat{\theta} : L \to L$ which extends θ. In particular we get $\widehat{\theta}(\alpha) = \theta(\alpha) = \alpha'$, and for any $c \in F$ we have $\widehat{\theta}(c) = \theta(c) = c$, so $\widehat{\theta} \in \mathrm{Emb}_F(L, L)$ has the desired properties.

(d) Suppose $\alpha \in E$. Prove that $m_{\alpha,F}(x)$ factors as a product of degree 1 polynomials in $E[x]$.

Let L be a splitting field for $m_{\alpha,F}(x)$ over E. We will show that all roots of $m_{\alpha,F}(x)$ in L actually lie in E. To this end, let $\alpha' \in L$ be a root of $m_{\alpha,F}(x)$; by part (c) we know that there exists some $\widehat{\theta} \in \mathrm{Emb}_F(L, L)$ such that $\widehat{\theta}(\alpha) = \alpha'$. But restricting the domain to E we have $\widehat{\theta}|_E \in \mathrm{Emb}_F(E, L)$, and then part (a) implies that $\widehat{\theta}|_E(E) = E$. In particular, because $\alpha \in E$ we find $\widehat{\theta}|_E(\alpha) \in E$, i.e. $\widehat{\theta}(\alpha) \in E$, and so $\alpha' \in E$ as desired.

3. Suppose E is a splitting field of $g(x) \in F[x] \setminus F$ over F. Suppose $E = F[\alpha]$ for some α. Prove that

$$|\mathrm{Emb}_F(E, E)| = \text{number of distinct zeros of } m_{\alpha,F}(x) \text{ in } E,$$

and deduce that $|\mathrm{Emb}_F(E, E)| \leq [E : F]$.

By Problem 2 we see that $m_{\alpha,F}(x)$ splits into linear factors in $E[x]$; it follows that E is a splitting field for $m_{\alpha,F}$ over F. Thus we can apply Problem 1 to find that

$$|\mathrm{Emb}_F(E, E)| = |\mathrm{Emb}_F(F[\alpha], E)| = \text{number of distinct zeros of } m_{\alpha,F}(x) \text{ in } E.$$

For the latter inequality we recall that $[F[\alpha] : F] = \deg(m_{\alpha,F})$. Thus we have

$$|\mathrm{Emb}_F(E, E)| = \text{number of distinct zeros of } m_{\alpha,F} \text{ in } E \leq \deg(m_{\alpha,F}) = [F[\alpha] : F] = [E : F].$$

4. Suppose p is prime and n a positive integer. Prove that

$$\mathrm{Emb}_{\mathbb{Z}_p}(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}) = \{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\}$$

where $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\sigma(a) := a^p$.

Notice that since $\mathbb{F}_{p^n}^\times$ is cyclic, there is $\alpha_0 \in \mathbb{F}_{p^n}$ such that $\mathbb{F}_{p^n}^\times = \langle \alpha_0 \rangle$. Hence $\mathbb{F}_{p^n} = \mathbb{Z}_p[\alpha_0]$. Therefore by Problem 3 we have $|\mathrm{Emb}_{\mathbb{Z}_p}(\mathbb{F}_{p^n}, \mathbb{F}_{p^n})| \leq [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n$. On the other hand we claim that $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ are all distinct elements of $\mathrm{Emb}_{\mathbb{Z}_p}(\mathbb{F}_{p^n}, \mathbb{F}_{p^n})$, which by the former inequality then implies these must be all the elements of $\mathrm{Emb}_{\mathbb{Z}_p}(\mathbb{F}_{p^n}, \mathbb{F}_{p^n})$. To see these elements are distinct, suppose $\sigma^i = \sigma^j$ for distinct $i, j \in \{0, 1, \ldots, n-1\}$, say without loss of generality $i < j$. Then we have that $\sigma^{j-i} = \mathrm{id}$, i.e. $\sigma^{j-i}(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$. This says that $\alpha^{p^{j-i}} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$, but then every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^{j-i}} - x$; this is impossible because $|\mathbb{F}_{p^n}| = p^n$ but this polynomial has at most $p^{j-i} < p^n$ roots. Thus $\sigma^i \neq \sigma^j$ and we get the result.

5. Suppose p is a prime. Let $E := \mathbb{Q}[\zeta_p, \sqrt[p]{2}]$ where $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$. Prove that $[E : \mathbb{Q}] = p(p-1)$.

We know the minimal polynomial of ζ_p over $\mathbb{Q}$ is $m_{\zeta_p,\mathbb{Q}}(x) = x^{p-1} + \cdots + x + 1$. Thus we have from lecture that $[\mathbb{Q}[\zeta_p] : \mathbb{Q}] = \deg(m_{\zeta_p,\mathbb{Q}}) = p - 1$. So from the tower $\mathbb{Q} \subseteq \mathbb{Q}[\zeta_p] \subseteq E$ we find using tower law that

$$[E : \mathbb{Q}] = [E : \mathbb{Q}[\zeta_p]]\,[\mathbb{Q}[\zeta_p] : \mathbb{Q}] = [E : \mathbb{Q}[\zeta_p]](p-1).$$

Furthermore, notice that $E = (\mathbb{Q}[\zeta_p])[\sqrt[p]{2}]$, and we know the minimal polynomial of $\sqrt[p]{2}$ over $\mathbb{Q}$ is $m_{\sqrt[p]{2},\mathbb{Q}} = x^p - 2$ (this is irreducible over $\mathbb{Q}$ by Eisenstein's criterion). Now by the defining property of the minimal polynomial, because $m_{\sqrt[p]{2},\mathbb{Q}} \in \mathbb{Q}[\zeta_p]$ vanishes at $\sqrt[p]{2}$ we must have $m_{\sqrt[p]{2},\mathbb{Q}[\zeta_p]}(x) | m_{\sqrt[p]{2},\mathbb{Q}}(x)$ in $(\mathbb{Q}[\zeta_p])[x]$, so as a result we find

$$[E : \mathbb{Q}[\sqrt[p]{2}]] = [(\mathbb{Q}[\zeta_p])[\sqrt[p]{2}] : \mathbb{Q}[\zeta_p]] = \deg(m_{\sqrt[p]{2},\mathbb{Q}[\zeta_p]}) \leq \deg(m_{\sqrt[p]{2},\mathbb{Q}}) = p.$$

Now returning to our first equality $[E : \mathbb{Q}] = [E : \mathbb{Q}[\zeta_p]](p-1)$ we have that $[E : \mathbb{Q}] \leq p(p-1)$ and also $p-1$ divides $[E : \mathbb{Q}]$. On the other hand we can consider the tower $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[p]{2}] \subseteq E$, and then applying the tower law in this scenario we find $[\mathbb{Q}[\sqrt[p]{2}] : \mathbb{Q}]$ divides $[E : \mathbb{Q}]$, and we know that $[\mathbb{Q}[\sqrt[p]{2}] : \mathbb{Q}] = \deg(m_{\sqrt[p]{2},\mathbb{Q}}) = p$, so p divides $[E : \mathbb{Q}]$. Putting this all together see that p and $p-1$ both divide $[E : \mathbb{Q}]$, which implies $p(p-1)$ divides $[E : \mathbb{Q}]$, and on the other hand we have seen that $[E : \mathbb{Q}] \leq p(p-1)$, so we get the equality $[E : \mathbb{Q}] = p(p-1)$.

10. Week 10

2. Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) = \mathbb{Z}_n^\times$.

We will define a map $f : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \to \mathbb{Z}_n^\times$. First recall that $\Phi_n(x) = \prod_{1 \leq i \leq n, \gcd(i,n)=1}(x - \zeta_n^i)$. So if $\theta \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$, then because θ must map roots of Φ_n to roots of Φ_n we must have $\theta(\zeta_n) = \zeta_n^i$ for some $i \in \mathbb{Z}$ with $\gcd(i,n) = 1$. We then define $f(\theta) = [i]_n \in \mathbb{Z}_n^\times$ (notice we are not imposing the restriction $1 \leq i \leq n$, we are allowing i to be any integer for which $\theta(\zeta_n) = \zeta_n^i$ holds). To show this is well-defined, we notice that if $\zeta_n^i = \zeta_n^j$ then $i \equiv j \pmod{n}$. We claim that f is a homomorphism. To show this, suppose $\theta, \sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$, say with $\theta(\zeta_n) = \zeta_n^i$ and $\sigma(\zeta_n) = \zeta_n^j$. Then notice that

$$(\theta \circ \sigma)(\zeta_n) = \theta(\sigma(\zeta_n)) = \theta(\zeta_n^j) = \theta(\zeta_n)^j = (\zeta_n^i)^j = \zeta_n^{ij},$$

and thus we have $f(\theta \circ \sigma) = [ij]_n = [i]_n[j]_n = f(\theta)f(\sigma)$, showing f is a homomorphism. Notice that if $\theta \in \ker(f)$ then this means $f(\theta) = [1]_n$, so $\theta(\zeta_n) = \zeta_n$ but then $\theta = \mathrm{id}$, so f is injective. For surjectivity notice for any $1 \leq i \leq n$ with $\gcd(i,n) = 1$ we have that ζ_n^i is a root of Φ_n, and so because Φ_n is irreducible in $\mathbb{Q}[x]$ we get that there is an isomorphism $\theta : \mathbb{Q}[\zeta_n] \to \mathbb{Q}[\zeta_n^i] = \mathbb{Q}[\zeta_n]$ such that $\theta(\zeta_n) = \zeta_n^i$, and then θ is an element of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$ satisfying $f(\theta) = [i]_n$, showing surjectivity.

Using the results of Lecture 24, we can prove the surjectivity as follows: As $x^n - 1$ has distinct zero in its splitting filed over $\mathbb{Q}$, it is a separable polynomial of $\mathbb{Q}[x]$. Since $\mathbb{Q}[\zeta_n]$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$ and $x^n - 1$ is a separable element of $\mathbb{Q}[x]$, $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])| = [\mathbb{Q}[\zeta_n] : \mathbb{Q}]$. We have proved that $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n) = |\mathbb{Z}_n^\times|$. Since the give group homomorphism $f : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \to \mathbb{Z}_n^\times$ is injective and the domain and the codomain have the same number of elements, we deduce that f is an isomorphism.

3. Prove that $\mathrm{Aut}_{\mathbb{Q}[\zeta_n]}(\mathbb{Q}[\sqrt[n]{2}, \zeta_n])$ is isomorphic to a subgroup of $\mathbb{Z}_n$.

We will define a map $f : \mathrm{Aut}_{\mathbb{Q}[\zeta_n]}(\mathbb{Q}[\sqrt[n]{2}, \zeta_n]) \to \mathbb{Z}_n$ as follows: notice that $\sqrt[n]{2}, \zeta_n \sqrt[n]{2}, \ldots, \zeta_n^{n-1} \sqrt[n]{2}$ are the roots of $x^n - 2$ in $\mathbb{Q}[\sqrt[n]{2}, \zeta_n]$ we know that for any $\theta \in \mathrm{Aut}_{\mathbb{Q}[\zeta_n]}(\mathbb{Q}[\sqrt[n]{2}, \zeta_n])$ we must have $\theta(\sqrt[n]{2}) = \zeta^i \sqrt[n]{2}$ for some $i \in \mathbb{Z}$ and then we define $f(\theta) = [i]_n \in \mathbb{Z}_n$. Similarly to part (a) we have that this is well-defined; to see it is a homomorphism, suppose we have $\theta, \sigma \in \mathrm{Aut}_{\mathbb{Q}[\zeta_n]}(\mathbb{Q}[\sqrt[n]{2}, \zeta_n])$, say $\theta(\sqrt[n]{2}) = \zeta_n^i \sqrt[n]{2}$ and $\sigma(\sqrt[n]{2}) = \zeta_n^j \sqrt[n]{2}$. Then we calculate

$$(\theta \circ \sigma)(\sqrt[n]{2}) = \theta(\sigma(\sqrt[n]{2})) = \theta(\zeta_n^j \sqrt[n]{2}) = \theta(\zeta_n^j)\,\theta(\sqrt[n]{2}) = \zeta_n^j\,(\zeta_n^i \sqrt[n]{2}) = \zeta_n^{i+j} \sqrt[n]{2},$$

where we use the fact that $\theta(\zeta_n^j) = \zeta_n^j$ because θ is $\mathbb{Q}[\zeta_n]$-linear. As a result we have

$$f(\theta \circ \sigma) = [i+j]_n = [i]_n + [j]_n = f(\theta) + f(\sigma).$$

To see that f is injective, notice that if $\theta \in \ker(f)$ then $\theta(\sqrt[n]{2}) = \sqrt[n]{2}$ and then because $\theta(\zeta_n) = \zeta_n$ (because θ is $\mathbb{Q}[\zeta_n]$-linear) we conclude $\theta = \mathrm{id}$. Now because the kernel is trivial we have by the first isomorphism theorem $\mathrm{Aut}_{\mathbb{Q}[\zeta_n]}(\mathbb{Q}[\sqrt[n]{2}, \zeta_n]) \simeq \mathrm{Im}(f)$ which is a subgroup of $\mathbb{Z}_n$.

4. Suppose n is a positive integer and p is a prime which does not divide n. Suppose $E_{n,p}$ is a splitting field of the n-th cyclotomic polynomial $\Phi_n(x)$ over $\mathbb{Z}_p$. Let $\alpha \in E_{n,p}$ be a zero of $\Phi_n(x)$.

   (a) Prove that the multiplicative order of α is n.

   Notice $\alpha^n = 1$ because $\Phi_n(x) | x^n - 1$. Let $d := o(\alpha)$ which we know must divide n, and suppose $d < n$. Then α is a root of $x^d - 1$, but we have the analagous factorization

   $$x^d - 1 = \prod_{k|d} \Phi_k(x),$$

   and thus $\Phi_k(\alpha) = 0$ for some $k|d$. Notice then $k|n$ but $k \neq n$ since $d < n$. In the factorization

   $$x^n - 1 = \prod_{d'|n} \Phi_{d'}(x)$$

   we see that α occurs both as root of $\Phi_n(x)$ and $\Phi_k(x)$; since these are distinct factors, we see that α is a repeated root of $x^n - 1$, which we claim cannot occur. The formal derivative of $x^n - 1$ is nx^{n-1}, and that $n \neq 0$ since $p \nmid n$. Thus $\gcd(x^n - 1, nx^{n-1}) = 1$, for instance this can be seen by writing

   $$(n^{-1}x)(nx^{n-1}) - (x^n - 1) = 1,$$

   where we've used the fact that $p \nmid n$ to see that $n \in \mathbb{Z}_p^\times$. Thus $x^n - 1$ does not have repeated roots so we have a contradiction.

   (b) Prove that $E_{n,p} = \mathbb{Z}_p[\alpha]$ and it is a splitting field of $x^n - 1$ over $\mathbb{Z}_p$.

   We know from part (a) that $o(\alpha) = n$. Thus $1, \alpha, \cdots, \alpha^{n-1}$ are all distinct elements of $E_{n,p}$, and they are all roots of $x^n - 1$, and hence these are all the roots of $x^n - 1$. Thus a splitting field of $x^n - 1$ over $\mathbb{Z}_p$ is given by $\mathbb{Z}_p[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}] = \mathbb{Z}_p[\alpha]$.
   Notice that since $\Phi_n(x) | x^n - 1$, all the zeros of $\Phi_n(x)$ in $E_{n,p}$ are of the form α^i for some i. Therefore $E_{n,p} \subseteq \mathbb{Z}_p[\alpha]$. On the other hand, $\alpha \in E_{n,p}$ which implies that $\mathbb{Z}_p[\alpha] \subseteq E_{n,p}$. Altogether we deduce that $E_{n,p} = \mathbb{Z}_p[\alpha]$, which completes our solution.

   Alternatively we can prove that $\Phi_n(x) = \prod_{\alpha' \in E_{n,p}, o(\alpha') = n} (x - \alpha')$ and use this to show that $E_{n,p} = \mathbb{Z}[\alpha]$: Recall from group theory because $o(\alpha) = n$ we have $o(\alpha^i) = n \iff \gcd(i, n) = 1$. For each such i, the element α^i having order n implies that α^i is a root of $\Phi_n(x)$ (it must be a root of $\Phi_d(x)$ for some $d|n$, and if it were a root of $\Phi_d(x)$ for $d < n$ then we could conclude it is also a root of $x^d - 1$, contradicting that $o(\alpha^i) = n$). Thus the elements $\{\alpha^i \mid 1 \leq i \leq n-1, \gcd(i, n) = 1\}$ are all roots of $\Phi_n(x)$, and because there are $\phi(n)$ such elements and $\deg(\Phi_n) = \phi(n)$, we see these are all the roots of $\Phi_n(x)$. Because $E_{n,p}$ is a splitting field of $\Phi_n(x)$ over $\mathbb{Z}_p$ we then have

   $$E_{n,p} = \mathbb{Z}_p[\{\alpha^i \mid 1 \leq i \leq n-1, \gcd(i, n) = 1\}] = \mathbb{Z}_p[\alpha],$$

   which proves the first claim (and we proved the second claim above).

   (c) Prove that $|E_{n,p}| = p^k$ where k is the multiplicative order of p in $\mathbb{Z}_n^\times$.

   We prove that $\mathbb{F}_{p^k}$ is a splitting field of $x^n - 1$ over $\mathbb{Z}_p$; by uniqueness of splitting fields we then conclude (using the result from part (b) as well) $E_{n,p} \simeq \mathbb{F}_{p^k}$ and we get the result. For the claim, notice that $p^k \equiv 1 \pmod{n}$, so $n | p^k - 1 = |\mathbb{F}_{p^k}^\times|$, and thus there is a subgroup $H \leq \mathbb{F}_{p^k}$ of order n (we use for this the fact that $\mathbb{F}_{p^k}^\times$ is cyclic). If we write $H = \{\alpha_1, \ldots, \alpha_n\}$, notice

every element of H is a root of $x^n - 1$ by Lagrange's theorem, so we get the factorization $x^n - 1 = (x - \alpha_1) \cdots (x - \alpha_n)$ in $\mathbb{F}_{p^k}[x]$, and then a splitting field of $x^n - 1$ over $\mathbb{Z}_p$ is given by

$$E := \mathbb{Z}_p[\alpha_1, \ldots, \alpha_n] \subseteq \mathbb{F}_{p^k}.$$

We claim that this inclusion is an equality: notice that we must have $|E| = p^\ell$ for some $1 \leq \ell \leq k$, and because $H \subseteq E^\times$ we must have by Lagrange's theorem that $|H| = n$ divides $|E^\times| = p^\ell - 1$. But then we see that $p^\ell = 1$ in $\mathbb{Z}_n^\times$, and this gives a contradiction if $\ell < k$ (because k is exactly the order of p in $\mathbb{Z}_n^\times$). Thus $\ell = k$, so $E = \mathbb{F}_{p^k}$ and we have the result.