HOMEWORK 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.

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.

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 $A^\times \times B^\times$.

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.

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

(In a unital commutative ring A, we say $a \in A$ is a *unit* if it has a multiplicative inverse. That means a is unit if there is $a' \in A$ such that $aa' = 1_A$. This is defined in the third lecture.)

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 $\mathbb{C}$.)

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.

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.

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 $\mathbb{Z}_p$.

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 $\mathbb{Q}[\sqrt{5}]$.

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

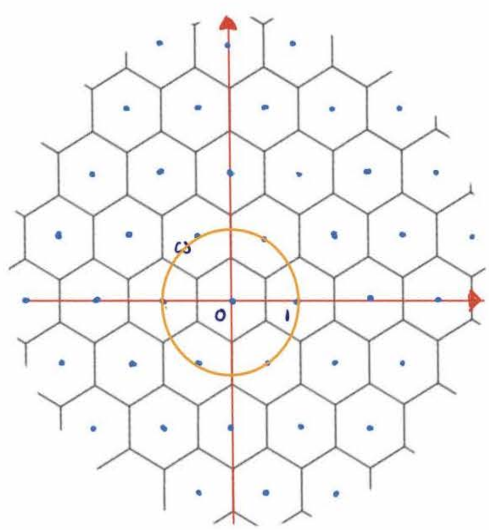
2. Find a zero of $x^3 - 2x + 1$ in $\mathbb{Z}_5$ and express is as a product of a degree 1 and a degree 2 polynomial.

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 $[0, p-1]$.

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

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.

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 $a_n \in \mathbb{Z}_m^\times$.

2. Let

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

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 $\ker \phi_{-1} = \langle x + [1]_3\rangle$.
(b) Prove that $\ker \psi = \langle x + 1, 3\rangle$. (Notice that here $1 = [1]_6$ and $3 = [3]_6$.)
(c) Prove that $\ker \psi = \langle 2x - 1\rangle$.
(d) Prove that $\mathbb{Z}_6[x]/\langle 2x - 1\rangle \simeq \mathbb{Z}_3$.
(e) Explain why $|\mathbb{Z}_6[x]/\langle 2x - 1\rangle| = 3 \neq 6^1$ does not contradict the first problem.

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

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 $p(x)$.

5. Suppose p is a prime more than 3 and $p = a_0^2 - a_0 b_0 + b_0^2$ 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 $p | a_0 + b_0 e$.
(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 $a_0 + b_0\omega \in \ker f$.
(c) Use the fact that $\mathbb{Z}[\omega]$ is a PID, and prove that $\ker f = \langle a_0 + b_0\omega\rangle$.
(d) Prove that

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

5. Week 5

1. Let $I := \langle x, y\rangle \lhd \mathbb{C}[x, y]$.
(a) Prove that I is a maximal ideal of $\mathbb{C}[x, y]$.
(b) Prove that I is not principal.

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 $D^\times = \{-1, 1\}$.
(b) Prove that $\sqrt{-21}$ is irreducible in D.
(c) Show that $D/\langle\sqrt{-21}\rangle$ is not an integral domain.
(d) Deduce that D is not a PID.

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

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

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

6. Week 6

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

2. Let $\alpha := \sqrt{1+\sqrt{3}}$. Find 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 $\mathbb{Z}[x]$.

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 $h(x)^2 - 1$.)

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 $\mathbb{Z}_p$.
   (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).
   (c) Prove that $\alpha^{p^n} = \alpha$. (Hint: for $\alpha \neq 0$, consider the group $F^\times$ of units of F.)
   (d) Prove that $f(X)|X^{p^n} - X$ in $\mathbb{Z}_p[X]$.

7. Week 7

Going through the proof of Eisenstein's irreducibility criterion one can see that the same argument works for polynomials with coefficients in a UFD. That means that the following holds: suppose D is a UFD, $p \in D$ is prime, and $f(x) := c_n x^n + \cdots + a_0 \in D[x]$ satisfies the following property:

$$p \nmid c_n, p|c_{n-1}, \ldots, p|c_0, \text{ and } p^2 \nmid c_0.$$

Then $f(x)$ cannot be written as a product of two smaller degree polynomials in $D[x]$. You are allowed to use this result for this week's HW assignment.

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

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

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

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

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

8. Week 8

1. This is an exercise from math100a which gives us a characterization of cyclic groups.
   (a) Suppose $C_n := \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order n. Show that if $d|n$, then C_n has exactly $\phi(d)$ elements that have order d. Use this to deduce that
   $$\sum_{d|n} \phi(d) = n.$$
   (b) Suppose G is a finite group and for every positive integer d,
   $$|\{g \in G \mid g^d = 1\}| \le d.$$
   Prove that G is cyclic. (Hint. Let $\psi(d)$ be the number of elements of G that have order d. Show that if $o(g) = d$, then $1, g, \ldots, g^{d-1}$ are all the elements of G that satisfy $x^d = 1$. Use this to deduce that if $\psi(d) \neq 0$, then $\psi(d) = \phi(d)$. Argue why we have $\sum_{d|n} \psi(d) = n$ where $n = |G|$. Use the first part to obtain that $\psi(d) = \phi(d)$ if $d|n$, and 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 $|F| \equiv 1 \pmod 4$.

3. Suppose F is a splitting field of $x^n - 1$ over $\mathbb{Z}_3$.
   (a) Find $|F|$ if $n = 3$.
   (b) Find $|F|$ if $n = 13$.
   (c) Find $|F|$ if $n = 39$.

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 $\theta_j(\zeta_p) = \zeta_p^j$.
   (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 $[1, p-1]$.

9. Week 9

In this problem set, we use the following notation. Suppose E and L are field extensions of F. Let
$$\mathrm{Emb}_F(E, L) := \{\theta : E \to L \mid \theta \text{ is an } F\text{-linear injective ring homomorphism}\}.$$
By F-linear, we mean $\theta(c) = c$ for every $c \in F$.

1. Suppose F is a field and $f(x) \in F[x]$ is irreducible. Let E be a splitting field of f over F. Let $\alpha \in E$ be a zero of f. Prove that
   $$|\mathrm{Emb}_F(F[\alpha], E)| = \text{number of distinct zeros of } f \text{ in } E.$$

2. Suppose F is a field, and E is a splitting field of a $g(x) \in F[x] \setminus F$ over F.
   (a) Suppose L is a field extension of E. Prove that, for every $\theta \in \mathrm{Emb}_F(E, L)$, $\theta(E) = E$. (Hint: Argue that all the zeros of g in L are in E and θ permutes them.)

(b) Suppose $\alpha \in E$, and let L be a splitting field of $m_{\alpha,F}(x)$ over E. Prove that 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 $\widehat{\theta}(\alpha) = \alpha'$.

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

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 $|\mathrm{Emb}_F(E,E)| \le [E:F]$.

4. Suppose p is prime and n is 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 $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \sigma(a) := a^p$.

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

10. Week 10

In this problem set, for a field extension E of F, we let
$$\mathrm{Aut}_F(E) := \{\theta : E \to E \mid \theta \text{ is a ring isomorphism, and } F\text{-linear}\}.$$

1. Prove that $\mathrm{Aut}_F(E)$ is a group under composition of functions.

2. Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \simeq \mathbb{Z}_n^\times$. (Hint: Use an argument similar to Problem 4, HW 8, and cyclotomic polynomials.)

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

4. Suppose n is a positive integer and p is 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 Φ_n in $\mathbb{Z}_p$.
   (a) Prove that the multiplicative order of α is n; that means $\alpha^n = 1$ and $\alpha^d \ne 1$ for positive integers d that are smaller than n. (Hint. Use $\prod_{d|n} \Phi_d(x) = x^n - 1$ and argue why $x^n - 1$ does not have multiple roots in its splitting field over $\mathbb{Z}_p$.)
   (b) Prove that $E_{n,p} = \mathbb{Z}_p[\alpha]$ and it is a splitting field of $x^n - 1$ over $\mathbb{Z}_p$.
   (c) Prove that $|E_{n,p}| = p^k$ where k is the multiplicative order of p in $\mathbb{Z}_n^\times$.

5. Suppose n is a positive integer.
   (a) Suppose, for some integer a, p is a prime factor of $\Phi_n(a)$ which does not divide n. Prove that $p \equiv 1 \pmod{n}$ and $\gcd(p,a) = 1$. (Hint: Use Problem 4(b) and show that $E_{n,p} = \mathbb{Z}_p$. Then use Problem 4(c).)
   (b) Prove that there are infinitely many primes in the arithmetic progression $\{nk+1\}_{k=1}^\infty$. (Hint: suppose $p_1, \ldots, p_k$ are the only primes in this arithmetic progression. Since $\Phi_n(np_1 \cdots p_k x)$ is not a constant polynomial, $\Phi_n(np_1 \cdots p_k a) \ne \pm 1, 0$ for some integer a. Hence there is a prime factor p of $\Phi_n(np_1 \cdots p_k a)$. Use Part (a) to deduce that p is different from p_i's and $p \equiv 1 \pmod{n}$.)