Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Solutions for Problem Sets 1 and 2

1 Gaussian Integers

1. Pair each of $1, \ldots, p-1$ with its inverse mod p. Then only 1 and $p-1$ are paired with themselves. Thus $1 \cdots (p-1)$ can be rewritten as $1 \cdot (p-1)$ times the product of pairs xx^{-1}, and so is congruent to -1 modulo p.

2. In fact, every euclidean ring is a principal ideal ring, since any nonzero element of an ideal of minimal norm generates the ideal. In fact, we will show that every principal ideal ring R is factorial. To prove existence of prime factorization, pick α a nonzero element of R. If α generates a prime ideal, then α is irreducible and we are done. Otherwise, the ideal (α) is contained in a maximal ideal (β_1); write $\alpha = \beta_1\alpha_1$. If α_1 is irreducible, we are done again. Otherwise, (α_1) is contained in a maximal ideal (β_2), and we may put $\alpha_1 = \beta_2\alpha_2$. If this process stops at some point, we obtain a factorization of α into irreducibles. Otherwise, we obtain an increasing sequence $(\alpha) \subset (\alpha_1) \subseteq \cdots$ of ideals which does not terminate, contradicting the fact that every principal ideal ring is noetherian. Thus the process must stop somewhere, and prime factorizations exist. As for uniqueness, if $\alpha_1 \cdots \alpha_m = \beta_1 \cdots \beta_m$ is an equality of two products of irreducibles, then $\beta_1 \cdots \beta_m$ belongs to the prime ideal (α_1), so one of the β_i must be a multiple of α_1, say β_1. In fact, β_1 and α_1 must generate the same ideal, since both generate maximal ideals. Thus we can factor off α_1 from both sides and keep going.

3. One method is to start with x such that $x^2 + 1$ is divisible by p (which can be found by exhaustive search, or by taking $x \equiv ((p-1)/2)! \pmod{p}$), then compute a generator of $(p, x+i)$ by imitating the proof from lecture that the Gaussian integers form a euclidean ring. That is, given generators (α, β), replace them by (β, γ), where $\gamma - \alpha$ is a multiple of β and $|\gamma| < |\beta|$. If $\gamma = 0$ at some point, then β generates the ideal $(p, x+i)$, and if $\beta = a + bi$, then $a^2 + b^2 = p$.

4. I know, I know, you can do this without the Gaussian integers. So sue me. Anyway, x and y can't both be odd by mod 4 considerations, so assume x is odd and y is even. Factor $z^2 = (x+yi)(x-yi)$. Then the GCD of $x+yi$ and $x-yi$ divides both $2x$ and $2yi$. If x and y have a common divisor, so does z, contrary to assumption. Thus the GCD of $x+yi$ and $x-yi$ also divides 2, but since x is odd and y is even, $x+yi$ is coprime to 2. Thus $x+yi$ and $x-yi$ are relatively prime. That means, up to units, each one is a perfect square. That is, there exist u, v such that $x+yi = (u+vi)^2 c$ for some unit c. Since $(u+vi)^2 = u^2 - v^2 + 2uv$, x is odd and y is even, c must be 1 or -1. If $c = -1$, we can rewrite $-(u+vi)^2$ as $(-v+ui)^2$. So without loss of generality, assume $c = 1$; then $x = u^2 - v^2$, $y = 2uv$, and $z = u^2 + v^2$, as desired.

5. We use the norm $f(a + b\sqrt{2}) = |a^2 - 2b^2|$. (Note that the absolute value is needed in this case!) Clearly this norm is multiplicative. Now given $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$

6. Let $s(n)$ be the number of ways to write n as a sum of two squares (by which I'll mean the

number of solutions of $x^2+y^2=n$ over the rational integers); then $s(n)$ is equal to the number of Gaussian integers of norm n. In particular, if m and n are relatively prime, α runs over the Gaussian integers of norm m, and β runs over the Gaussian integers of norm n, then $\alpha\beta$ runs over the divisors of mn, but each divisor of mn shows up four times. (If a divisor shows up once as $\alpha\beta$, it shows up as $(\alpha i^m)(\beta i^{-m})$ for $m = 0, 1, 2, 3$.) Thus $4s(mn) = s(m)s(n)$.
Suppose $n = p^e$ for p a prime congruent to 3 modulo 4. Then p is a prime in the Gaussian integers, so if $n = \alpha\overline{\alpha}$, both of α and $\overline{\alpha}$ are divisible by $p^{e/2}$. This is impossible if e is odd, so in that case $s(p^e) = 0$; if e is even, then the only possible α are $p^{e/2}i^m$ for $m = 0, 1, 2, 3$. Thus in this case $s(p^e) = 4$.
Next, suppose $n = p^e$ for p a prime congruent to 1 modulo 4. Then p factors as $\alpha\overline{\alpha}$ for some prime α. If $n = \beta\overline{\beta}$, then β must be of the form $\alpha^l\overline{\alpha}^{e-l}i^m$ for $l \in \{0, \dots, e\}$ and $m \in \{0, 1, 2, 3\}$. In this case, $s(p^e) = 4(e + 1)$.
Putting it all together, we get for $n = \prod_i p_i^{e_i}$,

$$s(n) = 4\prod_i \frac{s(p_i^{e_i})}{4} = 4\prod_i \begin{cases} e_i + 1 & p_i \equiv 1 \pmod 4 \\ 0 & p_i \equiv 3 \pmod 4, e_i \equiv 1 \pmod 2 \\ 1 & p_i \equiv 3 \pmod 4, e_i \equiv 0 \pmod 2. \end{cases}$$

2 Number Fields

1. We start with the basis 1 and $\sqrt{D}$, which may or may not be integral. Note that $\mathrm{Trace}(1) = 1 + 1 = 2$ and $\mathrm{Trace}(\sqrt{D}) = \sqrt{D} + (-\sqrt{D} = 0$. Thus

$$\mathrm{Disc}(1, \sqrt{D}) = \det\begin{pmatrix} \mathrm{Trace}(1\cdot 1) & \mathrm{Trace}(1\cdot\sqrt{D}) \\ \mathrm{Trace}(\sqrt{D}\cdot 1) & \mathrm{Trace}\sqrt{D}\cdot\sqrt{D} \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D.$$

Recall that if m is the index, in the ring of integers, of the $\mathbb{Z}$-submodule generated by this basis, then m^2 divides the discriminant of the basis. Since we assumed D is squarefree, either the basis $1, \sqrt{D}$ is integral, or it generates a $\mathbb{Z}$-submodule of the ring of integers of index 2.
First suppose $D \equiv 1 \pmod 4$. In that case, $(1 + \sqrt{D})/2$ has minimal polynomial $x^2 + x + (1 - D)/4$, and so is an integer. The basis $1, (1 + \sqrt{D})/2$ generates a $\mathbb{Z}$-submodule between the ring of integers and $\mathbb{Z} + \mathbb{Z}\sqrt{D}$, but the index between these is 2 and $\mathbb{Z} + \mathbb{Z}\sqrt{D}$ has index 2 in $\mathbb{Z} + \mathbb{Z}(1 + \sqrt{D})/2$. Thus $1, (1 + \sqrt{D})/2$ is an integral basis.
Next, suppose $D \not\equiv 1 \pmod 4$. In this case, we claim $1, \sqrt{D}$ is already an integral basis; since the index of its $\mathbb{Z}$-span in the ring of integers is at most 2, it suffices to check that if a, b are not both even, then $(a + b\sqrt{D})/2$ is not an algebraic integer. In fact, it suffices to check this for $(a, b) = (1, 0), (0, 1), (1, 1)$. In these cases, the minimal polynomials of these are $x - 1/2$, $x^2 - D/4$, and $x^2 + x + (1 - D)/4$, none of which have integer coefficients. Thus $1, \sqrt{D}$ is an integral basis. In summary: an integral basis is given by

$$\begin{cases} 1, \frac{1+\sqrt{D}}{2} & D \equiv 1 \pmod 4 \\ 1, \sqrt{D} & D \not\equiv 1 \pmod 4. \end{cases}$$

2. First we compute $\mathrm{Trace}(1) = 3$, $\mathrm{Trace}(\sqrt[3]{2}) = 0$, $\mathrm{Trace}(\sqrt[3]{4}) = 0$. (Either add up the conjugates in $\mathbb{C}$ or write out the matrices by which these act on $\mathbb{Q}Q(\sqrt{3})$ as a $\mathbb{Q}Q$-vector

space.) Thus

$$\mathrm{Disc}(1, \sqrt[3]{2}, \sqrt[3]{2^2}) = \det \begin{pmatrix} \mathrm{Trace}(1 \cdot 1) & \mathrm{Trace}(1 \cdot \sqrt[3]{2}) & \mathrm{Trace}(1 \cdot \sqrt[3]{2^2} \\ \mathrm{Trace}(\sqrt[3]{2} \cdot 1) & \mathrm{Trace}(\sqrt[3]{2} \cdot \sqrt[3]{2}) & \mathrm{Trace}(\sqrt[3]{2} \cdot \sqrt[3]{2^2} \\ \mathrm{Trace}(\sqrt[3]{2^2} \cdot 1) & \mathrm{Trace}(\sqrt[3]{2^2} \cdot \sqrt[3]{2}) & \mathrm{Trace}(\sqrt[3]{2^2} \cdot \sqrt[3]{2^2}) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix} = -2^2 \cdot 3^3.$$

Thus the index of $\mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{2^2}$ in the full ring of integers is either 1, 2, 3 or 6.
We next check that the index is not divisible by 2. That is, we check that if a, b, c are rational integers, not all even, then $\alpha = (a + b\sqrt[3]{2} + c\sqrt[3]{2^2})/2$ is not an algebraic integer. One could do this by computing the minimal polynomials for all possible choices of $a, b, c \in \{0, 1\}$, but in this case there is a shortcut. If α is an algebraic integer, so is $\alpha\sqrt[3]{2^2} = b + c\sqrt[3]{2} + (a/2)\sqrt[3]{2^2}$, as then is $(a/2)\sqrt[3]{2^2}$. But the latter has minimal polynomial $x^3 - a^3/2$, which has integer coefficients only if a is even. Thus $(b\sqrt[3]{2} + c\sqrt[3]{2^2})/2$ must also be an integer; multiplying by $\sqrt[3]{2}$, we find that b must be even, then c.
Finally, we check that the index is not divisible by 3. Again, we must check that if a, b, c are rational integers, not all divisible by 3, then $\alpha = (a+b\sqrt[3]{2}+c\sqrt[3]{2^2})/3$ is not an algebraic integer. It suffices to check this for $a, b, c \in \{0, 1, 2\}$. Again, one can list all of the minimal polynomials of these elements, but one can also do a bit better. Note that if we put $\beta = 1 + \sqrt[3]{2}$ and $\gamma = 1 - \sqrt[3]{2} + \sqrt[3]{2^2}$, then $\beta\gamma = 3$. Now $\alpha\gamma = (a+2b-2c)/3 + (-a+b+2c)\sqrt[3]{2}/3 + (a-b+c)\sqrt[3]{2^2}/3$ is equal to an element of $\mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{2^2}$ plus $(a - b + c)(1 + \sqrt[3]{2} + \sqrt[3]{2^2})/3$. This can only be integral if $a - b + c$ is divisible by 3, since $1 + \sqrt[3]{2} + \sqrt[3]{2^2}$ has minimal polynomial $x^3 - 3x^2 - 3x + 1$ whose constant coefficient is not divisible by any cube.
We now know that if α is integral, then $a - b + c$ is divisible by 3. Next, suppose $c = 0$. Then Then $\alpha(1 + \sqrt[3]{2} + \sqrt[3]{2^2}) = (a + 2b)/3 + (b + a)\sqrt[3]{2}/3 + (b + a)\sqrt[3]{2^2}/3$ is integral, so $a + 2b$ is divisible by 3, which now implies $a = b = 0$. A similar argument applies if $a = 0$, or if $b = 0$. The only remaining cases are $a = c = 1, b = 2$ or $a = c = 2, b = 1$. These are equivalent: in the former, the minimal polynomial of α is $x^3 - x^2 - x - 1/3$, which is not integral.
We conclude $1, \sqrt[3]{2}, \sqrt[3]{2^2}$ is an integral basis.

3. From what we have shown in class, it suffices to check that the discriminant of the polynomial $P(x)$ equals the discriminant of the basis $1, x, \dots, x^{n-1}$. Let $r_1, \dots, r_n$ be the roots of $P(x)$ in $\mathbb{C}$, which are precisely the conjugates of x in $\mathbb{C}$. The discriminant of the basis $1, x, \dots, x^{n-1}$ is

$$(\det(r_i^{j-1})_{i,j=1}^n)^2 = \prod_{i<j}(r_i - r_j)^2$$

by the properties of the Vandermonde determinant. (See Neukirch, p. 11. One proof of the Vandermonde formula: view both sides as polynomials in the r_i, note that the determinant vanishes whenever $r_i = r_j$, then check that the coefficient of some monomial matches up.) The latter is precisely the discriminant of P.

4. One example is $P(x) = x^3 + 2x + 2$, which has discriminant -140. The proof that $1, x, x^2$ is an integral basis is similar to the argument given in problem 2.

5. Note $2\cos(2\pi/n) = \zeta_n + \zeta_n^{-1}$ and $2\sin(2\pi/n) = -i(\zeta_n + \zeta_n^{-1}$; since i, ζ_n and ζ_n^{-1} are algebraic integers, these combinations are too. From this representation, we also see that the conjugates of $\cos(2\pi/n)$ are all of the form $\cos(2\pi k/n)$. If $\cos(2\pi/n)$ were an algebraic

integer, its norm would be an integer; but the absolute value of the product of the conjugates is less than 1 for $n \geq 5$, contradiction. The argument for $\sin(2\pi/n)$ is similar.

6. The root of a polynomial P with algebraic integer coefficients is an algebraic number; let K be the number field generated by the roots and coefficients of P. The integrality of the root now follows from the fact that $\mathfrak{o}_K$ is integrally closed, which we checked in class.

3 Interlude on Symmetric Polynomials

1. Let d be a positive integer; we check that the homogeneous symmetric polynomial of degree d with integer coefficients can be written by integer polynomials in $\sigma_1, \ldots, \sigma_n$. We order the monomials $x_1^{e_1} \cdots x_n^{e_n}$ in lexicographic order. That is, if two monomials have different e_1, whichever has the bigger e_1 is the bigger of the two. If the e_1's are equal, compare e_2's, and so on.
Now given a homogeneous symmetric polynomial P with integer coefficients, let $cx_1^{e_1} \cdots x_n^{e_n}$ be the largest monomial in lexicographic order. In particular, we must have $e_1 \geq \cdots \geq e_n$, otherwise the monomial with the exponents sorted in order also appears and is larger in lexicographic order. Then $P - c\sigma_1^{e_1-e_2} \cdots \sigma_{n-1}^{e_{n-1}-e_n} \sigma_n^{e_n}$ is symmetric with integer coefficients, and its largest monomial is strictly smaller than that of P. Thus this process eventually stops at the zero polynomial, and P has been expressed as an integer polynomial in the σ_i.

2. We just give the argument for $\alpha+\beta$ here, as the argument for $\alpha\beta$ is similar. Let $\alpha_1, \ldots, \alpha_m$ be the conjugates of α in $\mathbb{C}$, and let $\beta_1, \ldots, \beta_n$ be the conjugates of β in $\mathbb{C}$. Let $P(x)$ be the polynomial $\prod_{i=1}^m \prod_{j=1}^n (x - \alpha_i - \beta_j)$. The polynomial $\prod_{i=1} m \prod_{j=1}^n (x - t_i - u_j)$ can be viewed as a symmetric polynomial in the u_j with coefficients in the ring $\mathbb{Z}[t_1, \ldots, t_m]$, so by the previous problem is a polynomial in the elementary symmetric functions of the u_i. But the coefficients of this polynomial are themselves symmetric functions of the t_i, so can be written as integer polynomials in the elementary symmetric functions of the t_i. Substituting $t_i = \alpha_i$ and $u_j = \beta_j$, the elementary symmetric functions of the t_i and u_j become the coefficients of the minimal polynomial of α and β, which are integers. Thus P becomes a monic polynomial with integer coefficients, so its root $\alpha + \beta$ is an algebraic integer.

4 Conjugates, Trace and Norm

1. Let $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Let

$$X^n + a_1 X^{n-1} + \ldots a_n$$

be the minimal polynomial of α over $\mathbb{Q}$. Since α is algebraic we may assume that $a_i \in \mathbb{Z}$. Let α_i be the conjugates of α, and let σ_k be the k^{th} symmetric polynomial. Using the triangle inequality, and the identity $|\alpha_i| = 1$, we conclude that

$$\|a_i\| = \|\sigma_k(\alpha_1, \ldots, \alpha_n)\| \leq \binom{n}{k}.$$

Since this bound depends only on n, we conclude that there can only be *finitely many* algebraic integers of degree n with this property, since there are only finitely many polynomials for each n satisfying the above bound. On the other hand, if α has this property, then so does α^k for every k. Thus $\alpha^i = \alpha^j$ for some $i \neq j$ and we conclude (since $\alpha \neq 0$) that α is a root of unity.

2. Let α be an algebraic number of degree d. Suppose that $\mathrm{Trace}(\alpha^n) \in \mathbb{Z}$ for all n. Let α_i for $i = 1, \ldots, d$ be the conjugates of α. Observe that symmetric polynomials (in α_i) may be expressed in terms of the "Newton polynomials", which are symmetric polynomials given by taking the sum of the k^{th} powers (i.e. $\sum \alpha_i^k$). This follows from the formal identity:

$$\exp\left(-\sum_{k=1}^{\infty} \frac{t^k}{k} \sum_{i=1}^{d} \alpha_i^k\right) = \exp\left(\sum_{i=1}^{d} \log(1 - t\alpha_i)\right) = \prod_{i=1}^{d} (1 - t\alpha_i)$$

In particular, the minimal polynomial of α has denominators bounded purely in terms of d, and so $c_d \cdot \alpha$ is an algebraic integer for some universal constant c_d. Applying the same argument to α^n for all n we conclude that $c_d \cdot \alpha^n$ is also an algebraic integer for all n. One may infer that α itself is algebraic in various ways. One such way is as follows. Suppose that $(\alpha) = \mathfrak{p}_1^{a_1} \ldots \mathfrak{p}_n^{a_n}$. We wish to prove that $a_i \geq 0$ for all i. If $a_i < 0$, then for $c_d \cdot \alpha$ to be integral we must have $c_d \in \mathfrak{p}_i^{-a_i}$. Applying the same argument to α^n we must have $c_d \in \mathfrak{p}_i^{-a_i \cdot n}$ for all n, which is a contradiction. Alternatively, note that the $\mathbb{Z}$-submodule generated by $1, \alpha, \alpha^2, \ldots$ is finitely generated, since it's contained in the finitely generated $\mathbb{Z}$-module $c_d^{-1}\mathfrak{o}$, where $\mathfrak{o}$ is the ring of integers of $\mathbb{Q}Q(\alpha)$. That implies α is algebraic by a theorem from lecture.

5 Ideals and Unique Factorization

1. Let $R = \mathbb{Z}[\sqrt{-7}]$. Let $\eta = (2, 1 + \sqrt{-7})$. Then

$$\eta^2 = (4, -6 + 2\sqrt{-7}, 2 + 2\sqrt{-7}) = (4, 2 + 2\sqrt{-7}) = (2)(2, 1 + \sqrt{-7}) = (2)\eta.$$

Assuming unique factorization for ideals in R we conclude that $\eta = (2)$. Yet since the element $(1 + \sqrt{-7})/2 \notin R$, $(1 + \sqrt{-7})$ cannot lie in (2), and we are done.

2(i). Suppose first of all that there exists a solution to $x^2 = d \mod p$. Clearly we may take $2x \leq p$, and thus write $x^2 - d = pm$ with $m < p$. Let $\mathfrak{p}_1 = (p, x + \sqrt{d})$ and $\mathfrak{p}_2 = (p, x - \sqrt{d})$. We observe that

$$\mathfrak{p}_1\mathfrak{p}_2 = (p^2, p(x \pm \sqrt{d}), pm)$$

since $m < p$, $(m, p) = 1$ and so $(p^2, pm) = (p)$. Thus $\mathfrak{p}_1\mathfrak{p}_2 = (p)$. Observe that $\mathfrak{p}_1$ is not the unit ideal, since if $\mathfrak{p}_1 = (1)$ then by symmetry $\mathfrak{p}_2 = (1)$ and $(p) = \mathfrak{p}_1\mathfrak{p}_2 = (1)$. On the other hand, $\mathfrak{p}_1 \neq (p)$ since for $p > 2$, $(x + \sqrt{d})/p$ is not an algebraic integer (see previous assignment).

2(ii). In the other direction, suppose that $p\mathcal{O}$ is not prime in $\mathcal{O}$, and that p does not divide $2d$. Then we may write $(p) = \mathfrak{a}\mathfrak{b}$ with $\mathfrak{a}$ and $\mathfrak{b}$ neither (p) nor the unit ideal. Write $p = ab$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Since $\mathrm{N}(p) := \mathrm{Norm}(p) = p^2$, we must have $N(a)N(b) = p^2$. If $N(a) = 1$, then a is a unit and $\mathfrak{a}$ is the unit ideal. Thus $p | N(a)$, and similarly $p | N(b)$. Thus $N(a) = \pm p$. Write $a = x + y\sqrt{d}$, with $2x, 2y \in \mathbb{Z}$. Then

$$N(a) = x^2 - dy^2 = \pm p$$

Suppose that $p|y$. Then $p|x^2$, and thus $p|x$. This would imply, however, that $p^2|N(a) = \pm p$, which is clearly impossible. Thus p does not divide y. In particular, since $p \neq 2$, y is invertible modulo p, and $(xy^{-1})^2 \equiv d \mod p$, which was to be shown.

3. Suppose $\mathfrak{a}$ is an integral ideal which is not principal. Let α be a nonzero element of $\mathfrak{a}$ of minimum norm. By assumption, there exists $\beta \in \mathfrak{a} \setminus (\alpha)$. Choose $\gamma \in \mathbb{Z}[\sqrt{-5}]$ to minimize $|\delta|$, where $\delta = \beta/\alpha - \gamma$; then in particular, $\Re(\delta) \in [-1/2, 1/2]$ and $\Im(\delta) \in [-\sqrt{5}/2, \sqrt{5}/2]$. On the other hand, by assumption, $\delta\alpha = \beta - \gamma\alpha$ is a nonzero element of $\mathfrak{a}$, so $|\delta\alpha| \geq |\alpha|$, which is to say $|\delta| \geq 1$. Since $|\Re(\delta)| \leq 1/2$, it follows that $|\Im(\delta)| \geq \sqrt{3}/2$. Without loss of generality, assume $\Im(\delta) > 0$; then $\sqrt{3} - \sqrt{5} < \Im(2\delta - \sqrt{-5}) < 0$. If c is the closest integer to $\Re(2\delta)$, then put $\epsilon = 2\delta - \sqrt{-5} - c$; we have

$$|\epsilon|^2 \leq \Re(\epsilon)^2 + \Im(\epsilon)^2 \leq \frac{1}{4} + (\sqrt{3} - \sqrt{5})^2 < 1.$$

If $\epsilon \neq 0$, then $\epsilon\alpha$ is an element of $\mathfrak{a}$ of norm less than $|\alpha|$, contradiction. Thus $\epsilon = 0$ and so $2\beta \in (\alpha)$. Since this holds for all β, we conclude $[\mathfrak{a} : (\alpha)] = 2$ and that $2\mathfrak{a} \subseteq (\alpha)$.
Now let $\mathfrak{p} = (2, 1 + \sqrt{-5})$ and note that $\mathfrak{p}^2 = (2)$. That means that $(\alpha)|2\mathfrak{a} = \mathfrak{p}^2\mathfrak{a}$ and $\mathfrak{a}|(\alpha)$. That means that $\mathfrak{a}$ is either equal to $(\alpha), \mathfrak{p}^{-1}(\alpha)$ or $\mathfrak{p}^{-2}(\alpha) = (\alpha/2)$. The first and third choices are principal ideals, so we must have $\mathfrak{a} = \mathfrak{p}^{-1}(\alpha)$. Thus $\mathfrak{a}$ is in the ideal class of $\mathfrak{p}$, as desired.

4. Let I be an ideal in a Dedekind domain R. Let $a \in I$ be a non zero element. Then (a) is a non-trivial ideal in R, and by the hint in the exercise, R/a is a PID. On the other hand, since $(a) \subseteq I$, there is a commutative diagram:

$$R \longrightarrow R/a \longrightarrow R/I.$$

Let J be the kernel of $R/a \to R/I$. Since R/a is principal, we may write $J = b + aR$ in R/a, with $b \in R$. Thus $(a, b) = \mathrm{Ker}(R \to R/I) = I$. (This last claim could be expanded upon briefly, but it is completely trivial).

5. Since the group of ideals is generated by prime ideals, it suffices to prove the following statement for Dedekind domains: for any (non-zero) prime ideal $\mathfrak{p}$, there exists another ideal $\mathfrak{q}$ such that $\mathfrak{q}$ represents the same element of the class group of $\mathfrak{p}$, and $\mathfrak{q}$ is prime to any particular choice of finitely many ideals: $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$. Since R is a Dedekind domain, $\mathfrak{p}_i + \mathfrak{p}_j = R$ for all i, j. By the Chinese remainder theorem:

$$R/\mathfrak{p}^2\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n \simeq R/\mathfrak{p}^2 \oplus R/\mathfrak{p}_1 \oplus \ldots \oplus R/\mathfrak{p}_n.$$

In particular, since $\mathfrak{p} \neq \mathfrak{p}^2$, there exists an element $r \in R$ such that $r \in \mathfrak{p} \setminus \mathfrak{p}^2$, and $r \neq \mathfrak{p}_i$ for any i.
Let us consider the factorization of the ideal (r). By construction, the ideal $\mathfrak{p}$ occurs exactly once, and the ideals $\mathfrak{p}_i$ do not occur. Write $(r) = \mathfrak{p}\mathfrak{q}$. Then $\mathfrak{q}$ is prime to $\mathfrak{p}$ and $\mathfrak{p}_i$ for all i. On the other hand, $\mathfrak{q}$ is the *inverse* element to $\mathfrak{p}$ in the class group, since their product is principal. One finishes the proof by either taking some appropriate power of $\mathfrak{q}$ (since the class group is finite), or more appropriately, taking $N(\mathfrak{q})/\mathfrak{q}$, which is manifestly an integral ideal. (Or for a third argument, repeat the argument above with $\mathfrak{p}$ replaced by $\mathfrak{q}$, and $\mathfrak{p}_i$ replaced by $\mathfrak{p}_i \cup \mathfrak{p}$ to produce an ideal inverse to $\mathfrak{q}$ in the classgroup, and coprime to $\mathfrak{p}$ and $\mathfrak{p}_i$.)

6. We imitate the proof of Theorem I.3.1 in Neukirch; the key point is that $K[x]$ is a principal ideal domain. (Every nonzero ideal in $K[x]$ is generated by an element of minimum degree.) Let R be the integral closure of $K[x]$ in L. By Proposition 2.10, every ideal of R is a finitely generated $K[x]$-module, and hence is a finitely generated ideal. Thus R is noetherian. Moreover, since R is the integral closure of $K[x]$ in L, it is automatically integrally closed. (This was essentially a problem on the first homework; see also section 2 of Chapter 1 of Neukirch.) Now let $\mathfrak{p}$ be a nonzero prime ideal of R; it remains to show that $\mathfrak{p}$ must be maximal. For any $y \in \mathfrak{p}$ nonzero, there exists a polynomial $y^n + a_1 y^{n-1} + \cdots + a_n = 0$. Thus $a_n \in \mathfrak{p}$, so the intersection $\mathfrak{q} = \mathfrak{p} \cap K[x]$ is a nonzero ideal; it is also prime because $K[x]/\mathfrak{q}$ injects into $R/\mathfrak{p}$ and the latter is an integral domain. Thus $\mathfrak{q}$ is maximal, so $K[x]/\mathfrak{q}$ is a field and $R/\mathfrak{p}$ is an integral extension of $K[x]/\mathfrak{q}$. That forces $R/\mathfrak{p}$ to be a field: if $z \in R/\mathfrak{p}$ has minimal polynomial $z^m + b_1 z^{m-1} + \cdots + b_m$ over $K[x]/gothq$, then $b_m \neq 0$, so z is invertible. We conclude every nonzero prime ideal of R is maximal, so R is a Dedekind domain.